



# Disaster Recovery Plan



Library Reference Number: SYDR10001

Document Management System Reference: Disaster Recovery Plan

Address any comments concerning the contents of this manual to:

EDS Publications Unit  
950 North Meridian Street, Suite 1150  
Indianapolis, IN 46204  
Fax: (317) 488-5376

*EDS is a registered mark of Electronic Data Systems Corporation.*

*CDT-3/2000 (including procedures codes, definitions (descriptions) and other data) is copyrighted by the American Dental Association. ©1999 American Dental Association. All rights reserved. Applicable Federal Acquisition Regulation System/Department of Defense Acquisition Regulation System (FARS/DFARS) Apply.*

CPT codes, descriptions and other data only are copyright 1999 American Medical Association (or such other date of publication of CPT). All Rights Reserved. Applicable FARS/DFARS Apply.



## ***Revision History***

<b>Document Version Number</b>	<b>Revision Date</b>	<b>Revision Page Number(s)</b>	<b>Reason for Revisions</b>	<b>Revisions Completed By</b>
Version 1.0	April 23, 2003	All	New Document	Ronald Koger
Version 2.0	October 2003	All	Updated Styles	EDS Publications
Version 3.0	August 2004	All	Update Document	Leo Dabbs



## Table of Contents

<b>Revision History .....</b>	<b>iii</b>
<b>Section 1: Disaster Recovery Plan Overview .....</b>	<b>1-1</b>
Introduction .....	1-1
EDS Business Continuity Policy .....	1-1
Scope .....	1-1
Objectives .....	1-2
Assumptions and Limitations .....	1-2
Executive Summary .....	1-3
<b>Section 2: Crisis Management .....</b>	<b>2-1</b>
Emergency Action Responses .....	2-1
How to Use This Manual .....	2-3
What to do first .....	2-3
How to Notify the Initial Response Team .....	2-4
Criteria for Declaring a Disaster .....	2-5
Initiate Disaster Response .....	2-6
Assembling the Contingency Management Teams .....	2-7
<b>Section 3: Disaster Recovery .....</b>	<b>3-1</b>
Overview .....	3-1
Operating Environment .....	3-1
UNIX .....	3-1
Local Area Network .....	3-1
Database Administration .....	3-2
Alternate Site Specifications .....	3-6
System Recovery .....	3-7
Telecommunications .....	3-7
Applications .....	3-8
Indiana interChange Support .....	3-8
Finance .....	3-8
Provider Enrollment .....	3-9
Resolutions and Adjustments .....	3-9
Manual Processing .....	3-10
Claims .....	3-10
Claims Imaging .....	3-11
Data Entry .....	3-11
Output Processing .....	3-11
Logistical Support .....	3-13
Client Services .....	3-13
Systems Unit .....	3-15
Electronic Solutions Help Desk .....	3-15
Home and Community Based Services Waiver .....	3-16
Long Term Care .....	3-17
Managed Care .....	3-18
Third Party Liability .....	3-19
Office Equipment Recovery .....	3-19
<b>Section 4: Resumption of Normal Business .....</b>	<b>4-1</b>
Overview .....	4-1
Operating Environment .....	4-1
UNIX .....	4-1
Local Area Network .....	4-1

Database Administration .....	4-2
System Overview .....	4-2
Cycle Recovery Process .....	4-5
Telecommunications .....	4-6
Applications .....	4-6
Indiana interChange Support.....	4-6
Finance.....	4-7
Provider Enrollment.....	4-7
Resolutions and Adjustments .....	4-8
Manual Processing .....	4-9
Claims .....	4-9
Data Entry .....	4-10
Output Processing.....	4-10
SunPrint Server (199.42.137.71).....	4-10
Xerox Elixir Forms PC .....	4-10
Xerox Dig path PC/Scanner Station (199.42.136.16) .....	4-11
Blue Server / Streamweaver PC (199.42.136.18) .....	4-11
Xerox High Speed Printer Hardware .....	4-11
PB Series 8 400R .....	4-12
PB Series 8 600R (machine 2) .....	4-13
Paragon Mailing Machine .....	4-13
Data-card.....	4-13
Customers .....	4-14
Logistical Support .....	4-15
Client Services .....	4-15
Electronic Solutions Help Desk .....	4-17
Home and Community Based Services Waiver .....	4-18
Long Term Care .....	4-19
Managed Care .....	4-20
Third Party Liability.....	4-21
Office Equipment Recovery.....	4-22
<b>Section 5: Business Continuity Plan Maintenance.....</b>	<b>5-1</b>
Distribution of the Plan .....	5-1
Updating the Plan .....	5-1
Approval of the Plan.....	5-1
Testing the Plan .....	5-1
<b>Section 6: Contacts .....</b>	<b>6-1</b>
Initial Response Team .....	6-1
Crisis Management Team.....	6-1
EDS Corporate Crisis Management Office .....	6-2
Contingency Management Teams .....	6-2
EDS Support Organizations .....	6-3
EDS Security .....	6-4
Building Security and Maintenance .....	6-4
Local Authorities and Emergency Services.....	6-4
Public Utilities .....	6-5
Suppliers and Vendors.....	6-5
Rental Contacts .....	6-6
Mailing Service Contacts .....	6-6
Lodging Contacts .....	6-6
Medical Contacts.....	6-7
Transportation Contacts .....	6-7
Communications Contacts.....	6-7

Document Control Contacts .....	6-8
<b>Section 7: Forms and Tools.....</b>	<b>7-1</b>
Description of Contents .....	7-1
Business Continuity Self Assessment.....	7-2
Business Area Risk Assessment .....	7-10
Business Impact Matrix .....	7-13
Business Impact Scale 1-5 (Example).....	7-14
Dynamic Risk Factor (Sample).....	7-14
Critical Business Process Worksheet .....	7-15
Initial Assessment Checklist.....	7-16
Applications Assessment.....	7-17
Manual Processing Assessment.....	7-18
Operating Environment Assessment .....	7-19
Output Processing Assessment.....	7-22
Building Assessment .....	7-23
Chemical and Biological Agent Procedures .....	7-25
Immediate Response .....	7-25
Warning Signs.....	7-25
Anthrax - Center of Disease Control (CDC) Guidelines.....	7-25
Threat and Vulnerability Worksheet .....	7-29
Part 1–Identify Risks.....	7-29
Part 2–Evaluate Risks .....	7-29
Community Resources Worksheet .....	7-30
Customer Meeting Topics .....	7-31
Crisis Management Plan Outline.....	7-32
Employee Communication Procedure .....	7-33
Employee Contact Sheet.....	7-34
Employee Recovery Needs Assessment.....	7-35
Team Safety Assessment.....	7-36
General Items .....	7-36
Evacuations .....	7-36
Training Topics .....	7-37
Problem Log .....	7-38
Public Relations Guidelines .....	7-39
Recovery Plan Outline.....	7-40
Recovery Planning Team .....	7-41
Recovery Strategy Meeting Agenda.....	7-42
Recovery Team Responsibilities .....	7-43
Service Provider Questions .....	7-44
Telecommunications Services .....	7-45
Test Plan – Executive Summary.....	7-47
Test Results Report .....	7-48
<b>Appendix A: Memo of Understanding .....</b>	<b>A-1</b>
<b>Appendix B: Back-ups and Offsite Storage.....</b>	<b>B-1</b>
Excerpted from section 4.5.5 of EDS contract .....	B-1
Excerpted from section 5.4.14 of EDS contract .....	B-1
<b>Appendix C: Site Risk Analysis.....</b>	<b>C-1</b>
Overview .....	C-1
Threat/Vulnerability Worksheet .....	C-1
Facility Location .....	C-3
Building Construction .....	C-4
Communication Service Lines .....	C-4

Natural Hazards .....	C-4
Earthquakes .....	C-5
Volcanoes .....	C-6
Floods .....	C-6
Thunderstorms .....	C-10
Winter Storms .....	C-13
Tornadoes .....	C-14
Technological Hazards .....	C-19
Hazardous Materials .....	C-19
Universal Hazards .....	C-24
Utility Problems .....	C-24
Power Fluctuations .....	C-26
Structural Fires .....	C-27
Civil Disturbances .....	C-33
Conventional or Nuclear Attack .....	C-33
Computer Resource Failures .....	C-34
File Server Head Crash .....	C-34
Employee Accidents .....	C-34
Sabotage .....	C-34
Bomb Threats .....	C-36
Total Destruction .....	C-37
<b>Appendix D: Disaster Recovery Agreement .....</b>	<b>D-1</b>
<b>Appendix E: Disaster Recovery Project Plan .....</b>	<b>E-1</b>
<b>Appendix F: Severity 1 Systems .....</b>	<b>F-1</b>
<b>Glossary .....</b>	<b>G-1</b>
<b>Index .....</b>	<b>I-1</b>

## Section 1: Disaster Recovery Plan Overview

---

### Introduction

The service that EDS provides to its clients is fundamental to its client's business success. In addition, it is important to recognize that in the Digital Economy, a client's information is one of its most valuable assets and protecting it is of paramount importance. EDS' clients and shareholders entrust EDS to take proactive measures to safeguard their business information, processes, and assets in the event of a business crisis or disaster. The purpose of the EDS Business Continuity Policy is to establish EDS' guiding principles of Business Continuity for its clients, its business, and its employees.

### EDS Business Continuity Policy

*It is EDS' Business Continuity Policy to protect its employees, the information and assets entrusted to it by its clients, and the information and assets owned by EDS. Business Continuity includes the assessment of risk posed to critical business processes and the development, testing, maintenance, and implementation of Business Continuity plans that meet the clients' requirements and business needs as defined within mutual, contractual commitments. To accomplish this, EDS will proactively employ plans, processes and tools to reduce the likelihood or severity of a business disruption, a system outage, or the impact and duration of recovery from a disaster.*

The content of each Disaster Recovery Plan differs based on the type of service being addressed, but the standard categories are as follows:

- Operating Environment
- Manual Processing
- Telecommunications
- Output Processing
- Applications
- Logistical Support

*Business Continuity* is an essential business function, not just a technical exercise. Planning for the management of personnel, system and business disruptions, as well as the full recovery of critical technical systems and processes, is not a matter of *if*, but *when*. The serious implication of business continuity planning requires continued enthusiastic participation and commitment from EDS' leaders and employees as well as clients' leaders and employees, and in some instances suppliers, to ensure success. As EDS expands its presence in the global marketplace, it must continue to ensure its clients' and EDS' personnel, business processes, internal information and assets are protected and that it has clear, well-rehearsed business continuity plans. Commitment to and participation in business continuity planning is paramount to clients' and EDS' business success and the safety of employees and the work environment.

### Scope

The scope of this *Business Continuity Plan* is to document the tools, resources, and processes used to protect employees, information, and assets supported by the EDS Indiana Title XIX account located at 950 N. Meridian St. in Indianapolis.

Print operations services for various other EDS accounts are also provided by the EDS Indiana Title XIX account. Disaster recovery and resumption of normal business operations plans for these services are included as part of this document.

## Objectives

The objectives of the *Business Continuity Plan* are as follows:

- To provide a central repository for all documentation related to the business continuity process so these materials may be readily identified and used in the event of a disaster.
- To provide tools, forms and guidelines to assist in the construction of the Business Continuity Plan so relevant issues are identified and addressed.
- To provide tools, forms and guidelines to assist during an actual disaster so the recovery process can be completed in an orderly and timely fashion.
- To identify all resources that may be used in the event of a disaster so the appropriate information, personnel, and equipment can be quickly located and applied to the recovery process.
- To document a Crisis Management strategy so business interruptions or emergency situations are dealt with in such a manner as to minimize their impact on the organization.
- To document a Disaster Recovery Plan so essential business functions can be restored in the shortest amount of time possible.
- To document Resumption of Normal Business Plan so all regular business activities can be resumed in an orderly fashion after a disaster.
- To provide a mechanism for the ongoing maintenance and support of the Business Continuity Plan itself so the plan is kept up to date and could therefore be used during an actual disaster.
- To satisfy EDS Corporate requirements to address Disaster Recovery and Business Continuity issues so standards set forth in the EDS Business Continuity Policy are met.
- To satisfy the contractual responsibilities EDS has to its Indiana Title XIX client by minimizing the effects of a disaster through the use of a documented process to restore normal business operations after a disaster has occurred.
- To develop an awareness of the business continuity process among the personnel supporting the EDS Indiana Title XIX account so appropriate procedures will be used in the event of a disaster.

## Assumptions and Limitations

The *EDS Indiana Title XIX Business Continuity Plan* is based on the following assumptions or limitations:

- EDS and the client will agree upon a maximum allowable downtime, and use this limitation when making decisions about the appropriate strategy for recovery during service interruptions. The maximum downtime is 30 days, and is documented in the client's original Request For Proposal.
- The frequency of off-site data backup will be based upon the agreed to synchronization point for recovery and on the customer service level requirement for maximum lost data intervals. This is found in the EDS contract in *Sections 4.5 and 4.14*.
- Data communications can use diverse network routing, alternate routing, and/or diverse media where appropriate.

- Voice communications will be provided based on minimum functional requirements until normal service can be restored.
- When there is a complete loss of the local data center, recovery will be based on data stored off-site. For a partial loss, on site backups may be used.
- The location for coordinating recovery operations if the facility at 950 N. Meridian St. is destroyed is:

**Crosspoint  
9795 Crosspoint Blvd, suite 100  
Indianapolis, IN 46256**

- The applications required to sustain identified critical business processes will be recovered at an alternative site.

In the event a disaster is declared, the EDS Public Relations office receives all external inquiries related to EDS information processing services, received by telephone at XXX XXX XXXX or in person.

Inventories are not maintained for hardware and software purchased from EDS but owned by the customer; and these inventories are not part of this plan.

This Business Continuity Plan does not include recovery activities that are performed by the client or any other party outside of EDS unless specifically noted.

## Executive Summary

The purpose of the EDS Business Continuity Policy is to establish EDS' guiding principles of Business Continuity for its clients, its business, and its employees.

The *EDS Indiana Title XIX Business Continuity Plan* documents proactive measures taken at the account to safeguard client business information, processes, and assets in the event of a crisis or disaster. This plan details arrangements and procedures designed to minimize the impact of an event or respond to an event in such a manner that critical business functions continue with as little interruption or essential change as possible.

*Business Continuity Planning* is an encompassing term covering Crisis Management Planning, Disaster Recovery Planning, and Business Resumption Planning. The combination of these key business continuity functions provides advance arrangements and procedures that enable an organization to minimize the impact of an event or respond to an event in such a manner that critical business functions continue with as little interruption or essential change as possible. These three topics are all vital to the recovery process, and each describes a different phase within the overall Business Continuity Plan.

*Crisis Management* is the coordination of an organization's initial response to a business interruption or threat so that it is handled in an effectively and timely manner. Key areas within the Crisis Management phase include initial actions to address the immediate threat, followed by the notification of an appropriate Response Team. The Response Team investigates and assesses the threat or business disruption, applies predetermined standards to decide if a disaster has occurred, and then invokes the appropriate action plans to continue the recovery process into the next phase in the event a disaster is declared.

*Disaster Recovery* is the process by which predefined arrangements and procedures are initiated to enable an organization to respond to a declared disaster and resume critical business functions within a predetermined period. Disaster Recovery is not returning everything to a normal status. It is the

resumption of essential functionality at a minimal level, performed as quickly as possible. In this phase, some service to the client is restored to minimize loss and avoid further damage because of the disaster.

*Business Resumption Planning* is a process to develop arrangements and procedures designed to return the state of the business to normal operations. This involves a restoration of all products and services to a predisaster state and it may also involve dismantling any temporary measures undertaken in the crisis management and disaster recovery phases. The recovery process is complete, after the execution of the Business Continuity Plan.

The *EDS Indiana Title XIX Business Continuity Plan* contains seven different sections of documentation. The first section consists of introductory and definition documentation, including this Executive Summary. The next three sections are devoted to the Crisis Management, Disaster Recovery, and Business Resumption Plans described above.

The fifth section of the *EDS Indiana Title XIX Business Continuity Plan* consists of documentation related to its maintenance. It details the process for updating the approval process required for modifying the Business Continuity Plan. The section includes directions for testing the *Business Continuity Plan*.

The sixth section of the *Business Continuity Plan* contains contact lists that document names, phone numbers, and home addresses for everyone that might become involved in the disaster recovery process. These lists include EDS personnel (local and corporate), key clients, vendors, suppliers, landlords, local fire, police, and public utility departments, and so forth. The *Contacts* section lists the various Response and Recovery teams that execute various portions of the recovery process.

The last section of the *EDS Indiana Title XIX Business Continuity Plan* contains forms and tools. The *Forms and Tools* section contains documents to help plan and design the Business Continuity Plan. It also contains documents that are useful during the actual disaster recovery process.

The *EDS Indiana Title XIX Business Continuity Plan* is simple to use. When an individual becomes aware of a threat or potential disaster situation, they can reference the *Immediate Action* subsection *Section 2: Crisis Management*. Concise instructions for dealing with several emergencies are in this section, including directions indicating whom to notify. This section also contains instructions for the Initial Response Team that includes guidelines for assessing the situation, criteria for declaring a disaster, and procedures for initiating teams to begin the recovery process. Individuals encountering the threat or potential disaster situation who are unfamiliar with this process should review *Section 2: Crisis Management, How to Use This Manual*.

The Initial Response Team will use the *Business Continuity Plan* to initiate the appropriate recovery processes. These individuals will report to the Local Crisis Management Team.

## Section 2: Crisis Management

### Emergency Action Responses

Business disruptions can occur in many different forms. Sometimes it is a natural threat such as a tornado or a flood. Other times, it can be a threatened use of force or violence by a person or an organized group as a means of intimidating or coercing societies. Whether it is a natural threat or an act of terrorism, the emergency action list provides an individual with a plan of action to minimize the severity of the threat.

*Note: If a situation occurs during normal business hours (8 a.m. – 5 p.m., Monday - Friday) and it does **not** threaten the immediate health or safety of any individual, please contact an EDS manager or dial 0 and explain the situation to the EDS operator. They will initiate an appropriate response and notify the proper outside agencies.*

Table 2.1 – Emergency Notification List

Threat	Emergency Action	Notify
Bomb threat	Ask <u>someone else</u> to <b>dial 911</b> ; keep the person on phone as long as possible and collect as much information as possible. Use Bomb Threat Checklist located in <i>Section 7: Forms and Tools</i> .	Indianapolis Emergency Services at <b>911</b> ; Building Security at <b>XXX-XXX-XXXX</b> , and any EDS manager or any Initial Response Team member
Civil disturbance	Ensure all entrances and exits are closed and secure. Do not admit anyone without proper ID and authorization.	Indianapolis Emergency Services at <b>911</b> ; Building Security at <b>XXX-XXX-XXXX</b> , and any EDS manager or any Initial Response Team member
Computer crime	Immediately contact a member of the EDS management team or call EDS Corporate Security to report the incident.	Any EDS manager, any Initial Response Team member, or EDS Corporate Security at <b>XXX-XXX-XXXX</b>
Electricity/Power Outage	Check the computer room. If computer equipment is running but the air conditioning is not, notify any EDS manager or any member of the Initial Response Team.	Building Security at <b>XXX-XXX-XXXX</b> Any EDS manager or any Initial Response Team member
Explosion	<b>Activate a manual pull station fire alarm, if possible.</b> Vacate the building and proceed to your designated outside assembly area.	Indianapolis Emergency Services at <b>911</b> ; Building Security at <b>XXX-XXX-XXXX</b> , and any EDS manager or any Initial Response Team member
Fire	<b>Always activate a manual pull station fire alarm, if possible.</b> If the fire is small and contained and you feel comfortable doing so – use a fire extinguisher to put it out. Vacate the building and proceed to your designated outside assembly area.	Indianapolis Emergency Services at <b>911</b> ; Building Security at <b>XXX-XXX-XXXX</b> , and any EDS manager or any Initial Response Team member

Table 2.1 – Emergency Notification List

Threat	Emergency Action	Notify
Hardware malfunction or failure	Stop using the malfunctioning hardware.	Any EDS manager or any Initial Response Team member
Hazardous materials release	<b>Activate a manual pull station fire alarm, if possible.</b> Vacate the building and proceed to your designated outside assembly area.	Building Security at <b>XXX-XXX-XXXX</b> , and any EDS manager or any Initial Response Team member
Computer Room Ventilation or Air Conditioning Failure	If the computer room air conditioning is not running, notify any EDS manager or any Initial Response Team member.	Any EDS manager or any Initial Response Team member and Building Security at <b>XXX-XXX-XXXX</b>
Industrial espionage	Ensure all entrances and exits are closed and secure. Do not admit anyone without proper ID and authorization.	Any EDS manager, any Initial Response Team member, or EDS Corporate Security at <b>XXX-XXX-XXXX</b>
Injury or Illness	<b>Dial 911</b> to request ambulance or other emergency services. Notify Building Security so they can direct emergency personnel to correct floor and work area.	Indianapolis Emergency Services at <b>911</b> ; Building Security at <b>XXX-XXX-XXXX</b> , <b>Contact any EDS manager as quickly as possible</b>
Intrusion (unauthorized physical access)	Ensure all entrances and exits are closed and secure. Do not admit anyone without EDS ID badge.	Building Security at <b>XXX-XXX-XXXX</b> Any EDS manager or any Initial Response Team member
Malicious damage or destruction of property.	Ensure all entrances and exits are closed and secure. Do not admit anyone without EDS ID badge.	Building Security at <b>XXX-XXX-XXXX</b> or any EDS manager or any Initial Response Team member
Malicious damage, theft or destruction of software or data (including viruses)	Ensure all entrances and exits are closed and secure. Do not admit anyone without EDS ID badge.	Any EDS manager, any Initial Response Team member or EDS Corporate Security at <b>XXX-XXX-XXXX</b>
Organized labor dispute	Ensure all entrances and exits are closed and secure. Do not admit anyone without EDS ID badge.	Any EDS manager or any Initial Response Team member
Phone Outage	Report outage to any EDS manager or any Initial Response Team member.	Any EDS manager or any Initial Response Team member
Robbery – Direct confrontation by another person in building or immediate area.	<b>Dial 911</b> to request immediate response by law enforcement personnel. Notify Building Security; give them a description of the individual.	Indianapolis Emergency Services at <b>911</b> . Building Security at <b>XXX-XXX-XXXX</b> Any EDS manager or any Initial Response Team member
Sabotage	Report sabotage to any EDS manager or call EDS Corporate Security.	Any EDS manager, any Initial Response Team member or EDS Corporate Security at <b>XXX-XXX-XXXX</b>
Severe Weather	Move to a safe area, either an interior office or the elevator bank corridor.	Any EDS manager or any Initial Response Team member

Table 2.1 – Emergency Notification List

Threat	Emergency Action	Notify
Software failure	Report failure to any EDS manager or any Initial Response Team member.	Any EDS manager or any Initial Response Team member
Telecommunications failure	Report failure to any EDS manager or any Initial Response Team member.	Any EDS manager or any Initial Response Team member
Theft, Vandalism	Notify any EDS manager or Initial Response Team member.	Any EDS manager or any Initial Response Team member
Threatening Behavior- Verbal or Physical Threat of Violence	Notify any EDS manager or Initial Response Team member.	Any EDS manager or any Initial Response Team member
Water damage	Notify building security. If water damage is in the computer room, contact any EDS manager or Initial Response team member.	Building Security at <b>XXX-XXX-XXXX</b> Any EDS manager or any Initial Response Team member
Workplace violence / Physical Confrontation	Notify an EDS manager immediately. Contact Building Security and call <b>911</b> to request emergency assistance.	Indianapolis Emergency Services at <b>911</b> ; Building Security at <b>XXX-XXX-XXXX</b> , and any EDS manager or any Initial Response Team member
All Other Potential Disaster Situations	Take appropriate action to safeguard people, information, and assets.	Any EDS manager or any Initial Response Team member

## How to Use This Manual

A disaster is defined as any situation that causes or threatens to cause a business disruption or loss of service. It can also be defined as anything that threatens EDS employees or information and assets belonging to either EDS or its clients. Use the *EDS Indiana Title XIX Business Continuity Plan*, if a situation currently exists that may fit either of these definitions.

**The first priority should always be to ensure the safety and health of individuals in the immediate vicinity! DO NOT attempt to take any action that might place anyone in danger. Notifying others of the danger is urgent, and the first response should always be to warn others before taking any further action.**

Use this manual as a guideline and reference tool. The topic headings within this section of the manual outline the steps to initiate a response to a potential disaster. Subsequent sections of this manual include a list of the individuals who should be involved in the recovery process, a description of actions that may be necessary to recover emergency services immediately following a disaster, and a further set of actions required to resume normal business functionality.

## What to do first

If a disaster threatens the work environment, follow the steps below:

- Turn to *Section 2: Crisis Management*, pages 2-1 and 2-2. If any of the potential disaster scenarios listed describes your current situation, follow the Emergency Action Response instructions listed. Be sure to alert the appropriate contacts as soon as possible.

- If none of the disaster scenarios listed on pages 2-1 and 2-2 describe your current situation, take whatever action is appropriate to safeguard assets, information and EDS employees. Then notify a member of the Initial Response Team and/or a manager as soon as possible. *Section 6: Contacts*, starting on page 6-1 list the Initial Response Team members.

## How to Notify the Initial Response Team

Notify a member of the Initial Response Team immediately when a potential disaster condition is identified. Members of the local Initial Response Team are listed in *Section 6: Contacts*.

The Initial Response team should quickly obtain information about the potential disaster situation. The Initial Response Team should determine whether normal operating procedures are adequate to resolve the problem. If they are not, contact the Crisis Management Team. The Crisis Management Team will determine whether to declare a disaster and initiate the full recovery process documented within the *Business Continuity Plan*. The Crisis Management Team will also initiate the Response To Operational Problems (RTOP) process.

## Criteria for Declaring a Disaster

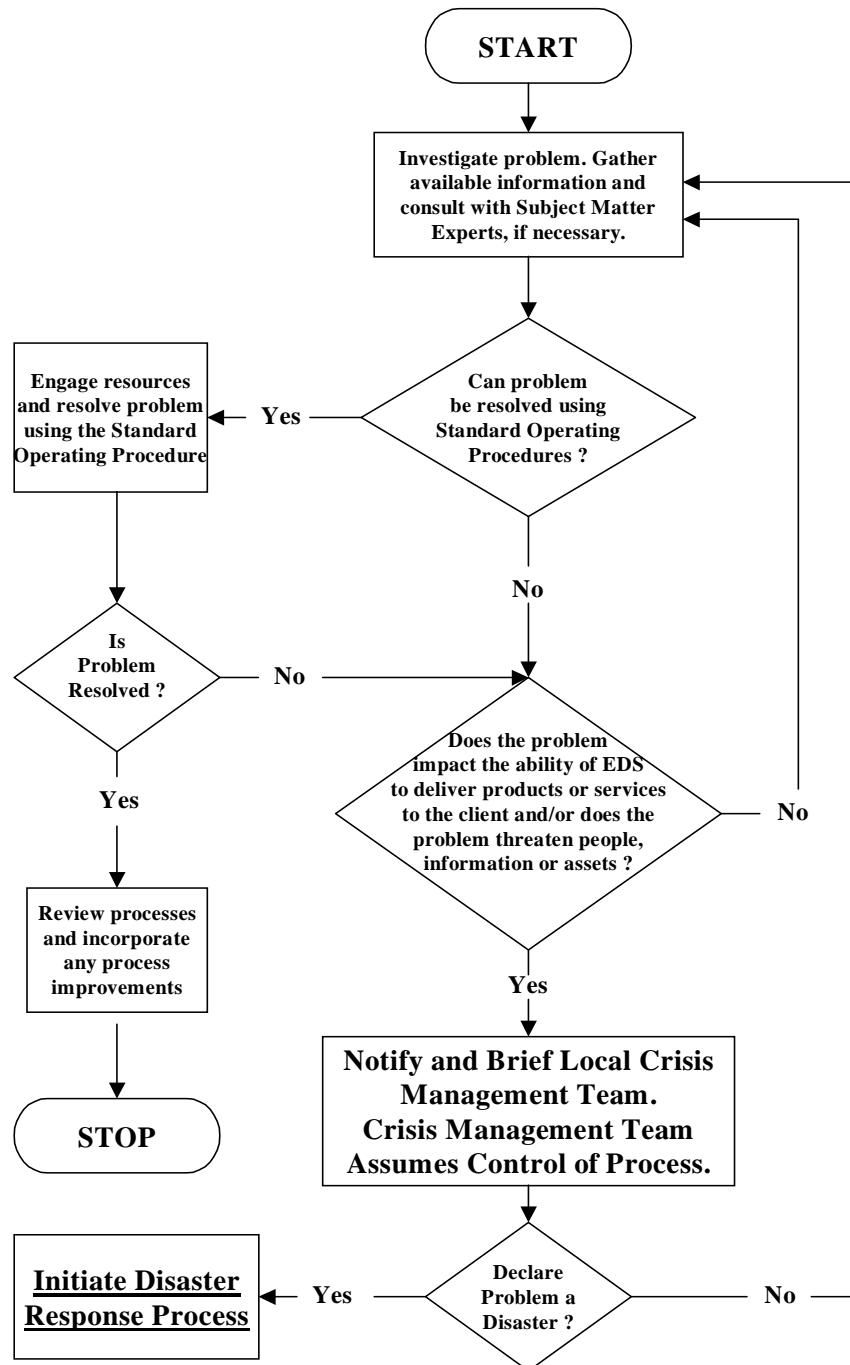


Figure 2.1 - Criteria for Declaring a Disaster

## Initiate Disaster Response

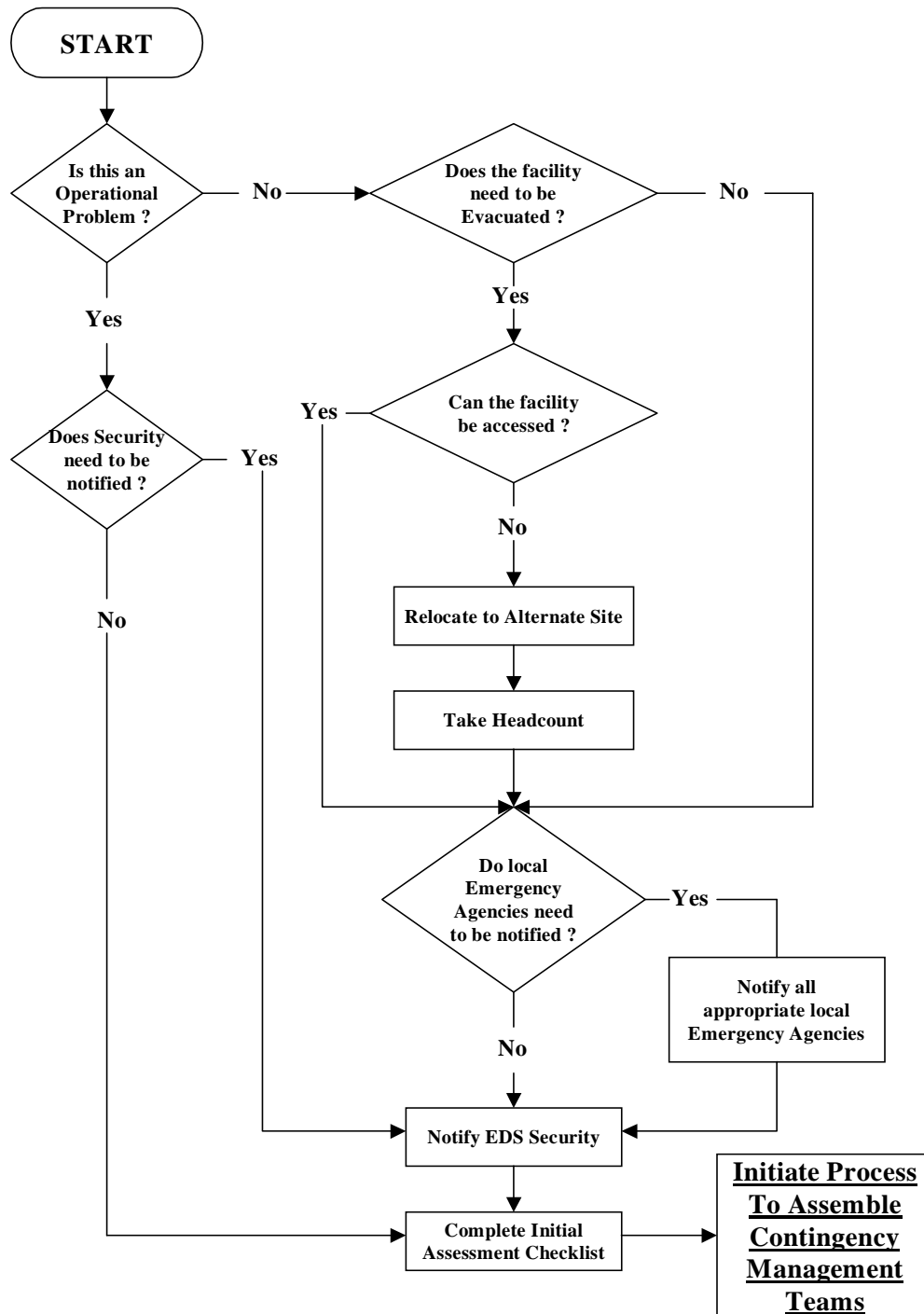


Figure 2.2 - Initiate Disaster Response

## Assembling the Contingency Management Teams

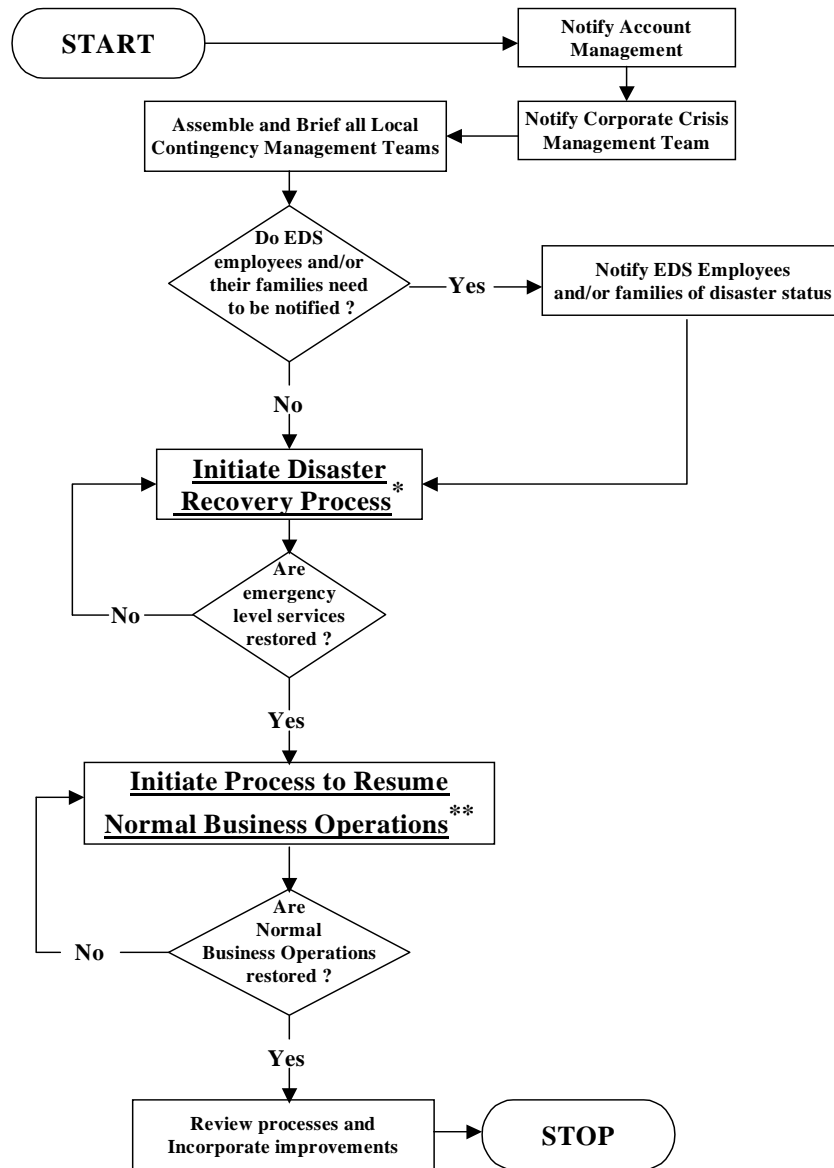


Figure 2.3 - Assembling the Contingency Management Teams

\* See Section 3 – Disaster Recovery

\*\* See Section 4 – Resumption of Normal Business



## Section 3: Disaster Recovery

---

### Overview

*Disaster Recovery* is the phase of the *Business Continuity Plan* that enables an organization to respond after a disaster by re-establishing identified critical business functionality. Disaster recovery plans are designed to restore essential services at a minimum level in the shortest amount of time. When these essential services have been restored, the disaster recovery effort continues with efforts to resume normal business functionality. *Section 4: Resumption of Normal Business* details that phase of the *EDS Indiana Title XIX Business Continuity Plan*.

### Operating Environment

Restoration of the EDS Indiana Title XIX operating environment during disaster recovery includes establishing a UNIX hardware platform, recovery of the Local Area Network, and recovery of critical databases. Documentation for these critical areas follows.

#### UNIX

Immediate action is necessary in the event of a disaster to resume Sun UNIX operations as quickly as possible. Use the resources located at the following address:

##### EDS

This location currently serves as the Indiana alternate processing center and has the hardware, software, and communication resources necessary to implement the disaster recovery phase.

Notify the on-call system administrator DSSC PACT SA Team using pager number XXX-XXX-XXXX.

The on-call system administrator will then contact the disaster recovery coordinator and Plano account manager.

Full backups of the Sun UNIX processing environment and documentation under the scope of these plans are currently stored at:

UNIX\_Plano\_DRA is the disaster recovery documentation for the Sun UNIX environment. This document has the procedures to restore data and bring all the equipment back online. The documentation is stored offsite in a permanent box at the Iron Mountain location listed above.

#### Local Area Network

To restore the local area network (LAN), including all security files and controls, the following actions must be performed.

1. Restore Servers
  - Obtain servers

- Restore the workgroup servers in the following order:
  - Domain controller(s)
  - Thin Client Server
  - Application Image Server
  - Document Management Server
  - Imaging Servers
  - All web servers

*Note: See Restoring the Os in the Backup/Restore section of the Infrastructure Manual.*

2. Restore connectivity:

- Obtain network hardware
- Establish Local Area Service
- Establish EDSLINK connectivity
- Establish foreign network connectivity

*Note: See Restoring Connectivity in the Infrastructure Manual.*

3. PC configuration and deployment:

- Obtain PC hardware
- Configure for user environment

*Note: See Desktop Configuration in the Infrastructure Manual.*

## **Database Administration**

**Oracle RDBMS**      The Oracle RDBMS application resides on DSIBSUN0 (all test databases, all model office databases, change management and document management), DSIBSUN1 (claim engine and autosys), DSIBSUN2 (production Indiana interChange DB), and DSIBSUN3 (history, Management and Administrative Reporting (MAR), business objects, and Decision Support System (DSS)).

**System Overview**      This plan covers the recovery of the production DBMS (Oracle) software and data located on DSIBSUN0, DSIBSUN1, DSIBSUN2, DSIBSUN3, and DSIBSUNB.

Recovery includes the following production databases, in order of priority:

1. INCEAP1
2. INECGP2
3. INAIMP1
4. INHISP1
5. INDOCP1 (contains Library and Claims Imaging information)

Recovery and restoration of all DBMS systems is completed at the local site when it is re-established.

### **DSIBSUN1**

**Sizing  
Requirements**

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*

- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*

**DSIBSUN1 Production Databases**

- INCEAP1 – 4.2 GB  
Claim Engine
- INJOBP1 – 735 MB  
Autosys Scheduler
- Two Log Files – 1GB each
- Checkpoint Space – 35 GB
- The SUN1 server runs the claim engine and the autosys scheduling software. The POS claims also process on this server.

**DSIBSUN2**

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*
- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*
- The SUN2 server runs the Indiana interChange online database and the Document Management and Claims Imaging database. A backup claim engine resides on this server. The flat history files are also stored on SUN2. The history files are used during the batch cycles.

**DSIBSUN2 Production Databases**

- INAIMP1 – 181 GB

Indiana interChange On-line

- INDOCP1 – 1.2 GB
- Two Log Files – 1GB each
- Checkpoint Space – 35 GB

**DSIBSUN3**

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*
- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*
- The SUN3 server houses the Decision Support System (DSS), Business Objects, Management and Administrative Reporting (MAR), and history databases.

**DSIBSUN3 Production Databases**

- INHISP1 – 414 GB

History

- Two Log Files – 1GB each
- Checkpoint Space – 35 GB

**DSIBSUNB**

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*
- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*
- The SUNB server houses the Production and Model Translator databases

**DSIBSUNB Production Databases**

- INECGP2 – 6 GB

## Production Translator

- Two Log Files – 1GB each
- Checkpoint space – 35 GB

*Note: SUN0, SUN1, SUN2, and SUN3 run the Solaris 2.6 operating system. The Oracle database is version 8.0.5. SUNB runs Solaris 8 operating system. The Oracle database is version 8.1.7.4.*

**Cycle Recovery Process**

Use the following steps to recover each database. Repeat these steps for each database restoration.

*Note: Refer to DBA Manual in Document-Prod library in INDOCPI for “how to” specifics.*

Environment variables required for production—defined by login file `/home/oracle/.profile`, `.kshrc`):

1. Verify recovery of the Solaris 2.6 platform (See *Systems Administrator's ADRP*).
2. Verify that the Legato Networker utility and the current Legato indexes have been restored.
3. Verify recovery of the password and group files (both NIS and local). Verify that Oracle and DSIBDBA IDs are defined in the local `/etc/passwd` file and the NIS password file.
4. Restore `/opt/???` and `/export/home/oracle` from the UNIX system back-up tapes. This restores only executables and other files, not the DB data files.
5. Determine the exact date and time required for database recovery. Each database can be recovered to a specific point in time as long as all data file locations and archive logs are available at the time the database backup was taken and ending with the required recovery time. This time must be coordinated to allow all database, system, and application files to be restored to the same point in time.
6. Restore all database files from the most recent back-up tapes. The back-up used must have been complete before the determined date and time. If the backup was still running at that time, use the back-up tapes from a previous backup. If the back-ups were taken while the database was up, back-up tapes and archive tapes are needed. If the back-ups were taken while the database was down, all tapes must be from the same backup.
7. Restore the database data files, archive logs, and control files. The log file that was current while the backup was being taken must be restored.
8. Install current version of Oracle software.
9. Verify all database row device locations were created at the correct size. Also, create directory structures for each database.

10. Verify all startup parameters are set up correctly in the *init.ora* files for each database and verify all database create scripts, and run to create new databases.
11. Restore all data files, redo logs, and control files to the correct locations. Begin individual database recovery processes.
12. Roll forward using archive logs to a specific point in time.
13. If necessary, change global netutil entries to correspond to the new database server. Use the *\$II\_SYSTEM/oracle/bin/netutil* utility.
14. Verify the creation of the database—run some test queries, run a batch job script to test remote access, run the UNIX online executable, run a Structured Query Language (SQL) query if a configured PC is available.

#### Backup Methodology

Daily system backups, which include database backups. The Tivoli Storage Manager backup software begins all backups automatically at 4 p.m. Eastern time.

Two types of backups occur during the week, incremental and full. Incremental backups are scheduled Monday through Friday. A full system backup is processed on Saturday and Sunday.

At the conclusion of all system backups, both incremental and full, the information is duplicated to another media set and sent to the off-site storage facility.

#### In-House Backup

Full backups and all other incremental backups are stored in an in-house tape library. A barrel lock controls access to the tape library, and only authorized personnel have access to the key. The tape library uses a barcode system. The backup software manages tape content. The UNIX administrator maintains the logs that indicate the system and backup tapes.

#### Off-Site Backup Retention

The duplicate media designated for off-site storage is placed into a container that is marked with the current date and container contents. The off-site delivery service picks up the container the first business day after the media is created and delivers it to the off-site storage location.

Upon receiving the container, the off-site storage vendor will catalog the container, and store it for future retrieval. By default all backup containers will automatically be returned to the INXIX processing site 30 days after they are received.

The address of the off-site backup retention location is:

The off-site storage facility houses electronic versions of the following:

- System backups

#### Backup and Job Restart Capabilities

IBM DB2/UDB maintains journal files of all transactions applied to the database since the associated backup. This allows the capability to restore the database at the time of the backup and roll those transactions forward that were committed up to the point of a disaster. If the journal files cannot be recovered, the database would be restored at the point of the latest full backup.

If a disaster occurred during a batch cycle, a determination would have to be made on whether to roll the database forward and restart the cycle at the point of the disaster or to start the cycle over as of the last database backup. The following are some of the factors to make a determination:

- Are the database journal files available?
- How much of the cycle has been completed?
- How long would it take to reach the completed point in the interrupted cycle?

- How long would it take to roll the database forward?

### **Alternate Site Specifications**

#### **Sun Mid-Range Platform**

The following lists the servers and applications loaded on each server.

Table 3.1 – Systems Overview

Server	Description	Application
DSDESUN5	Production Server	Solaris, X.25, CA-Unicenter, IBM DB2/UDB, Tivoli Storage Manager, ECMS, Tuxedo, IBM WebSphere MQ Series

The hardware configurations of each server are as follows.

Table 3.2 – Hardware Specification

Platform	Configuration	Operating System	CPU	Memory	Disk
DSDESUN5	Sun E5500	Solaris 2.8	8-333 MHz	6G	1TB

#### **System Application Requirements**

Operating System:

- Solaris v.2.8.0

Network Operating System:

- TCP/IP

System Software Required:

- Veritas Volume Manager v. 3.1.1

Other software required:

- MicroFocus COBOL v.3.1.35r-e
- Tivoli Storage Manager v.5.1.0.2
- Tuxedo v.6.1
- OpTech Sort v.1.7y (plus bug fixes)
- Solstice X.25 v.2.1
- CA-Unicenter v.1.5
- IBM DB2/UDB v.7.1 SP5
- WebSphere MQ Series 5.3.0

#### **Required Communications**

Unique hardware required:

AIT-II tape drives, modems

Current access methods:

- Ethernet connections using TCP/IP for PC
- Connection and servers connections

- Login capability through EDS\*LINK

Contingency access methods:

- Type 1 – EDS\*LINK Access
- Type 2 – Dial up/PPP via modems

## System Recovery

### Disaster Declaration

When a crisis occurs that requires use of the off-site location, the following steps must be accomplished in order to prepare for access to the facility:

1. Call the alternate site pager
2. When the call is returned, say “This is a disaster notification.”
3. Provide the following information:
  - Company name
  - Caller’s name
  - Telephone number where the caller can be reached
  - Nature of the disaster

There are dedicated positions at the alternate site for disaster coordination and planning. In the event of a real disaster, the first option is to have key account staff travel to the recovery site with some intermediate preparation by the staff at the alternate site while personnel, tapes, and so forth are transported to the alternate site. In the event the account staff is not available, EDS will provide staff at the alternate site to perform recovery procedures. Until the original site or a new primary site is established, the alternate site is to perform limited processing.

## Telecommunications

In the event of a disaster, immediate action must be taken to resume telecommunication services as quickly as possible. EDS facilities in Indianapolis currently occupied by the Indiana Solution Centre will be used as a temporary Disaster Recovery alternate work site. Voice and data communications for Indiana Title XIX personnel will have to be established at these sites.

To recover the Indiana Title XIX voice and data communications environment in case of a partial or total disaster, see the following documentation:

- Voice Network Recovery Plan
- Data/Network/Circuit Recovery Plan

These plans are currently stored in a permanent box at the following offsite location:

The documentation listed above contains key contact information, voice and data circuit information, and a list of critical phone numbers and T1 configuration information. The documents also outline procedures to restore data and voice communication and bring all required equipment back online.

## Applications

Restoration of the EDS Indiana Title XIX application environment during disaster recovery requires establishing the ability to support critical business and system functionality. In addition to direct technical support of the Indiana interChange application, the recovery of Finance, Provider Enrollment, and Resolutions and Adjustments are required to provide a minimal level of functionality.

### ***Indiana interChange Support***

To support the Indiana interChange system during this recovery effort, essential personnel must have access to the system running at the alternate/backup site. These personnel must inspect the system to ensure proper functionality has been restored. In addition, these personnel must have continued access in order to verify processing results, respond to client inquiries and correct any problems that may arise.

To provide this level of support, it is essential that temporary facilities be established to provide a normal work environment for 18 Systems Engineers. These facilities must contain PCs capable of accessing EDSNET and the public Internet, in addition to normal office equipment (desks, chairs, phones, copiers, fax machines, and so forth). Install the following software and hardware on the indicated number of PCs.

- PowerBuilder v 7.03 – 6 PCs
- LBMS client – 18 PCs
- Business Objects – 6 PCs
- Reflections – 18 PCs
- 56K V92 Modem – 1 PC

### ***Finance***

The Finance Unit consists of ten full time employees that perform the following tasks:

- MAR and CMS 64 Reporting
- Cash control
- Daily provider payment
- Document expenditures
- Daily funding of Medicaid
- Bank reconciliation and tax assessment reconciliation
- Tax assessments
- Expenditures
- Accounts receivables
- Repayment agreements
- Daily balancing and MAR reporting
- Premium vendor services

These tasks fall within the critical path for the processing and payment of claims, and are therefore vital to this account. EDS obtains funds from the State daily to reimburse for Medicaid claims paid that

day. It is required that these funds reach a zero balance each day, and failure to do so can jeopardize the entire claims payment process. EDS also performs premium vendor services for CHIP and MEDWORKS members and must be able to send invoices and collect premium payments daily. For this reason, it is critical that these ten performers regain the ability to perform duties as quickly as possible after a disaster.

The following are the emergency business needs for the Finance Unit following a disaster:

- Five PCs with EDSNET access to the Indiana interChange system, the Internet, On-Demand, IndianaAIM, DSS, Business Objects, Fifth Third Direct, and one PC must have access to MAR.
- Seven desks
- Seven phones
- One fax machine
- One copier
- Standard office supplies

## **Provider Enrollment**

The Provider Enrollment Unit performs most of its functions within the Indiana interChange system. The unit is unable to operate without access to interChange. In the event of a major business interruption, the Provider Enrollment Unit would become operational when interChange access is restored. This includes the hardware and linkage necessary to operate in the system. The Provider Enrollment Unit works closely with several other units on the account, including Managed Care, Operations, Finance, and Claims. These units would need to be operational as well for Provider Enrollment to operate normally. The unit's quality analyst produces reports for the State Office of Medicaid Policy and Planning (OMPP), on quality outcomes. As noted above, most of these reports rely on information contained in Indiana interChange.

The following are the emergency business needs for Provider Enrollment following a disaster:

- Two PCs
- Access to Indiana interChange
- Access to Provider file information
- Six desks
- Six phones

## **Resolutions and Adjustments**

The following are emergency business needs for Resolutions following a disaster for:

- Back up data in Indiana interChange to process claims.
- Five personal computers (PCs)
- Printers
- A copy of the *Claims Resolution Manual*
- Calculators
- Pens
- CRLD backup for reporting

- Back up reports and logs used for daily reporting
- Copies of Resolutions *Operating Procedures Manual*

The following are the emergency business needs for Adjustments following a disaster:

- Back up data in Indiana interChange to process Adjustments
- CRLD backup for reporting
- Back up reports and logs used for daily reporting
- Four PCs
- Printers
- Phones
- Calculators
- Pens
- Forms needed to process adjustments
  - Copies of *Adjustment Operating Procedures Manual*
  - Cabinets to store work

## Manual Processing

Manual Processing at the EDS Indiana Title XIX account is a critical business function. The contract with the client requires Indiana Title XIX to process IHCP paper claims in a timely fashion. In the event of a disaster, this functional area is a high priority. Manual processing requirements may be divided into two sub-categories: Claims and Data Entry.

### Claims

The following are emergency business needs for the Claims Unit following a disaster:

- All incoming P.O. Box mail must be delivered to the alternate work location.
- A standard office environment must be provided for the team.
- Specific office supplies are required. They include mail sorters, rubber bands, correction tape, highlighters, pens, pencils, letter openers, cabinets, tape, carts, staple pullers, rubber fingers, and rubber gloves.
- Other essential supplies are required. They include a letter-opening machine, microfilm machines, supplies for microfilm machine, PCs, printer, copier, microfilm, folders, Indiana interChange, and RTP Access database.
- A copy of the Claims Unit training manual must be available.
- Copies of all logs and reports used daily (batch header sheets, batch activation log sheets, microfilming process forms, production reports, production sheets, quality reports, quality sheets, status report, CPC 4, CPC 5, CPC 49, and CPC 16) must be available.
- Shelving must be available to keep all incoming claims for 90 days.
- Quality information must be collected for RFP requirements.
- All copies of claims on microfilm that are not at the warehouse must be moved to the alternate work location.

## **Claims Imaging**

- Need access to at least one (preferably 2) high speed scanner that has a minimum resolution of 200 dpi
- Need at least 14 PCs for imaging processing

## **Data Entry**

The Data Entry Unit is part of the Claims Department and is responsible for the correct entry of all manually processed claim data into *IndianaAIM*.

The following are emergency business needs for Data Entry following a disaster:

- One supervisor
- Four employees (three lead operators, one quality analyst)
- Back up Viking system to process claims
- Four terminals
- Data Entry training manual
- System and forms quality check claims to meet RFP requirements
- Shelves
- Balance log
- One PC with Microsoft Excel
- Five chairs
- Five desks
- Production sheets to record completed batches
- Calculator

## **Output Processing**

To restore the capabilities of the print center to its original functionality; the following items need to be performed.

1. Acquire Printer Hardware from Xerox
  - Two DocuPrint 180 with EPS front end
  - One DocuPrint 135 with LPS front end
2. Acquire Sun print servers
  - SparcUltra
3. Acquire PC hardware
  - Four PCs with Standard Windows Configuration
4. Restore Network Connectivity
  - Eight port hub with CAT5 cabling
  - Connect to Local Area Network as described in the Infrastructure Manual.
5. Restore software and electronic resources
  - Blue Server/Configuration files

- StreamWeaver/Configuration files
- DocUSP/Forms, Font, Image resources
- Elixir Desktop/Configuration files
- Adobe Acrobat
- Xerox LCDS Filter

*Note: See Restoring Print Room Environment in the Output Processing Disaster Recovery Manual.*

Table 3.3 lists the required product resources.

Table 3.3 – Required Product Resources

Product Name	Item #
8 1/2 x 11 bottom perf w/ cutter (4,000/box) (40skd)	SIS PERF - 001
4-across (4-up labels - 3 1/2 X 15/16)	9102
Voucher with label - X622 (3,000/box)	601-022
Voucher no label - X625	601-925
Allstate preprinted letterhead (roll feed) X195	500-195
Allstate Renewal Pink	AG80
Allstate May 2002 Policy Changes - Purple	AG83
Allstate Dwelling Policy Jackets	AP450-1
Allstate General Property Jackets	AP451-1
Allstate Residential Condo Policy Jacket	AP452-1
Allstate NJ Dwelling Policy Jackets	ANJ116
Allstate NJ General Property Jackets	ANJ117
Allstate NJ Residential Condo Policy Jackets	ANJ118
Nationwide Privacy Statement (July 1st)	G-9333-1
Nationwide Dwelling Policy Jacket	800-401
Nationwide General Property Jacket	800-402
Nationwide Residential Condo Policy Jacket	800-403
Travelers Dwelling Policy Jacket	TFP10
Travelers General Property Jacket	TFP11
Travelers Residential Condo Policy Jacket	TFP47
Travelers Transfer Bill Insert	TFP45
Travelers Privacy Insert	PL-10561
Omaha Dwelling Policy Jacket	601-401
Omaha General Property Jacket	601-402
Omaha Residential Condo Policy Jacket	601-403
Omaha Expired Agent - 1/3 Gray	601-431
Omaha Rollover Letter Ivory	601-432
Omaha Expiration Reissue Insured - 1/3 Aqua/Green	601-433
Omaha Expiration Reissue Agent - 1/3 Peach	601-434
Omaha Expiration Reissue Mortgage - 1/3 Blue	601-435
Omaha Privacy Notice	MC31063

Table 3.3 – Required Product Resources

Product Name	Item #
Omaha Flood Policy has Changed insert - 1/3 Gold	J1040
Tri-folded 8 1/2 X 11, Re-Inspection insert White	INSP10
1-window WHITE Remit Envelope (35) - 2,500/case	AU8
2-window WHITE - <b>IMPORTANT</b> Envelope (30)	AU9
2-window WHITE - Plain Envelope (30) - 2,500/case	AU9A
2 Window Kraft - 9 X 12 Envelope (500 / box)	601-310
Omaha #10 window envelope	601-302

**Inserting Recovery Plan:****Required Equipment:**

- PB Series 8 600R (machine 2) as configured above
- Back-up files of job modes
- SIS reconciliation spreadsheet
- Printer log sheets
- SIS tracking “L” report

**Logistical Support**

Logistical Support at the EDS Indiana Title XIX account consists of six areas. Client Services, Electronic Solutions Help Desk, HCBS Waiver and Hospice, Office Equipment Recovery, Managed Care, and Third Party Liability. The following lists the requirements for these areas.

**Client Services**

The client services director leads four business units within the Client Services department located on the 11<sup>th</sup> floor of 950 North Meridian Street, including Customer Assistance, Written Correspondence, Provider Enrollment, and Provider Assessment.

The four units share some tools, such as a fax machine and a LAN printer/copier with white paper, laminator, 3-hole punch, heavy-duty stapler, LAN I:drive, outlook (e-mail), office supplies, Internet access, and TV/VCR combo. In addition to each unit's individual needs, these shared tools are also necessary for the units to function. The four units also share EDS internal services, such as the courier service to HCE and the OMPP.

The following pages of requirements are unit-specific.

**Provider  
Representatives**

The contract requires EDS to retain representatives on staff to visit, educate, and answer questions for providers associated with the Indiana Health Coverage Programs. While the phone staff can answer most questions, some are more complex, or individualized questions, and are referred to the representative for that territory. Provider Representatives work both in and out of the office; have cell phones, laptops, and company vehicles. In the event of a disaster, it would not be likely that all of the aforementioned equipment would be lost.

The following are emergency business needs for Provider Representatives following a disaster:

- One supervisor
- Twelve representatives
- Twelve laptops and dialup access
- Twelve cell phones
- Ten cars
- Access to interChange and On-Demand
- Twelve provider manuals

**Customer  
Assistance (Phone  
staff)**

The contract requires EDS to answer provider and member calls for the IHCP within two minutes of calling into the queue between the hours of 8 a.m. and 12 p.m. and 1 p.m. and 5 p.m., Monday through Friday, excluding State holidays. For Premium Vendor Services, the hours are of 8 a.m. and 7 p.m., Monday through Friday, excluding State holidays. The phone staff uses 20 phones with headsets, computers, IndianaAIM, Web interChange, On-Demand, the provider manual, one telephone with taping capabilities, blank tapes, and copies of banner pages and bulletins to perform required duties. In the event of a disaster at 950 N. Meridian Street, the majority of equipment would be lost.

The following are emergency business needs for Customer Assistance following a disaster:

- One supervisor
- Ten phone staff
- Twelve desks, chairs, and PCs
- Twelve phones with headsets
- Access to interChange and On-Demand
- Toll free phone line service
- Thirteen provider manuals
- One telephone with recording capability
- One printer

**Written  
Correspondence**

The contract requires EDS to answer provider and member written requests for the Indiana Health Coverage Programs within 10 business days of receipt. The written correspondence staff uses five computers, Indiana interChange On-Demand, the provider manual, and copies of banner pages and bulletins to perform their job. In the event of a disaster at 950 N. Meridian Street, the majority of their equipment would be lost.

The following are emergency business needs for Written Correspondence following a disaster:

- One supervisor
- Four staff members
- Five desks, chairs, and PCs
- Access to interChange and On-Demand
- Five provider manuals, bulletins, and banner pages

## Systems Unit

### Account Services

The contract requires EDS to maintain the procedure code tables within Indiana interChange and answer questions about Indiana interChange edits and audits in the Indiana Health Coverage Programs. Account Services also researches why claims may not be processing correctly, and answers questions that the phone staff and field representatives cannot answer. Account services uses phones, computers, Indiana interChange, CRLD, and many HCPCS and CPT reference books.

The following are emergency business needs for Account Services following a disaster:

- Four staff members
- Four desks, chairs, and PCs
- Four telephones
- Access to interChange and CRLD
- Four provider manuals
- Six file cabinets

## Electronic Solutions Help Desk

The Electronic Solutions Help Desk provides telephone support for the following areas:

- Providers and clearinghouses sending or receiving electronic data
- Providers using the OMNI eligibility system
- Providers using EDS Web interChange
- EDS internal infrastructure helpdesk support

The help desk has a phone system with three separate incoming lines –ECS support at XXX-XXX-XXXX or toll free XXX-XXX-XXXX, OMNI system support at XXX-XXX-XXXX or XXX-XXX-XXXX, and internal infrastructure support at XXX-XXX-XXXX.

### Physical Set Up:

To establish a temporary site the following minimum equipment and supplies are necessary to accommodate responses to the provider/vendor community:

*Note: These estimates are based on requirements to provide essential services only during the first few days after a disaster.*

- Two support personnel
- One Omni device
- Two desks
- Two chairs
- Two PCs
- Two power surge protectors multiple Plug in capacity
- One modem
- Two phones with three lines each

- General office supplies – paper, pens, stapler, paper clips, and Julian calendar

**Communication Requirements:**

- Connection to Sun 5
- Connection to Sun 6
- Connection to Sun 0
- Connection to Internet – for web interChange
- Access to LAN

**Temporary Operations:**

The support personnel will receive and respond to incoming inquiries about the status of electronic claim submission and eligibility. Initial responses could be handled with the above-mentioned equipment. Additional equipment would be necessary within a few days to re-establish complete activity of the help desk.

***Home and Community Based Services Waiver***

The Home and Community Based Service (HCBS) waiver consists of 13 full time employees that perform the following tasks:

- One Clerical Support
- One Supervisor
- Eight HCBS Waiver Review Analysts
- Two Recoupment Analysts
- One Waiver Specialist

This response plan is based on the contract in year 2002. The Waiver Support position tasks fall within the critical path for the notification for scheduling all waiver reviews and the processing and payment of recoupments, and are therefore vital to continuing meeting RFP contractual obligations. The provider notification for waiver review is required two weeks before the scheduled review. It is critical that this one individual performer regain the ability to perform duties as quickly as possible after a disaster. This department's requirement for the Disaster Recovery Phase of the *Business Continuity Plan* is to have a standard office environment setup for one individual during the first week after the disaster.

The following are emergency business needs for HCBS following disaster:

- One PC with EDSNET access to the Indiana interChange SUR subsystem, Insite, and the ability to access the public internet
- Desk
- Phone
- Fax
- Copier
- Office supplies

The Indiana interChange SUR subsystem is critical for providing HCBS waiver teams the claims history reports for completing the contract-required reviews. There will be a CD file of all Waiver

forms housed off-site, with a copy of the response and recovery plan. The 10 review analysts, the supervisor, and waiver specialist would need to regain the ability to perform their duties two weeks post disaster. The setup would include 10 laptop computers, and six printers, four docking stations, and other office equipment considered normal in a standard business environment (desk, phone, fax, copier, office supplies, and so forth). Review teams are in the office one week per month. If the review teams are not in the office at the time of the disaster, this equipment would not be needed immediately. The review teams would need access to the unit L: drive with files restored, EDSNET, Indiana interChange, Insite database, and the public Internet. Additionally, the two waiver recoupment analysts would need PCs with access to Indiana interChange within two weeks post disaster. This will enable recoupments identified during the audits to be performed.

## **Long Term Care**

The Long Term Care Unit consists of 16 full-time employees:

- One director
- One supervisor
- Twelve Long Term Care Review Analysts
- One Statistical analyst
- One Clerical Support Staff

This response plan is based on the contract in year 2004. The LTC unit's responsibilities of auditing LTC facilities, and the compilation and reporting of data obtained during these audits, is a condition of meeting RFP contractual obligations. It is critical that one individual performer regain the ability to perform duties as quickly as possible after a disaster. This department's requirement for the Disaster Recovery Phase of the Business Continuity Plans is to have a standard office environment setup for one individual during the first week after the disaster.

The following are emergency business needs for LTC following disaster:

- One PC with access to Indiana*Aim* and MAR
- Desk
- Phone
- Fax
- Copier
- Office Supplies

There will be a CD file of all LTC forms housed off-site, with a copy of the response and recovery plan. The twelve review analysts would need to regain the ability to perform their duties two weeks post disaster. The setup would include thirteen laptop computers, which each analyst currently has in their possession, six printers, four docking stations, and other office equipment found in a standard business environment, such as desks, phones, fax machine, copier, and office supplies. Review teams are in the office throughout the week, and this equipment would be needed as soon as possible. The review teams would need access to the L Drive with files restored, EDSNET, Indiana*Aim*, and the public internet. Additionally, the two waiver recoupment analysts would need PCs with access to Indiana interChange within two weeks post disaster. This will enable recoupments identified during the audits to be performed.

## **Managed Care**

The Managed Care Unit performs most of its functions within the interChange system. The unit is unable to operate without access to interChange. In the event of a major business interruption, the managed care team would become operational when interChange access is restored. This includes the hardware and linkage necessary to operate in the system. The Managed Care Unit works closely with several other units on the account, including Provider Enrollment, Operations, and Claims. These units would need to be operational for Managed Care to operate normally. In addition, Provider Enrollment houses managed care enrollment paperwork. The majority of documentation could be lost or destroyed in a major disaster.

The following are emergency business needs for Managed Care following a disaster:

- Access to IndianaAIM
- One PC
- One telephone
- Printer connection
- One chair and work surface

## **Publications**

The contract requires EDS to maintain operating procedure manuals, provider manuals, user's guides, to produce periodic bulletins, and weekly banner pages to communicate with providers (and members) enrolled in the IHCP.

The Publications Unit uses telephones, PCs, and reference materials (including dictionaries, thesaurus', style guides, technical writing guides, and other reference manuals) to verify information used in the documents being written, edited, or reviewed. The Publications Unit uses Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Outlook, Microsoft Access, Adobe Acrobat, Internet Explorer, Indiana interChange, and Hummingbird DM.

The following are emergency business needs for Publications following a disaster:

- One supervisor
- Four employees
- Five desks
- Five chairs
- Five PCs, equipped with Microsoft Word, Microsoft Outlook, and Hummingbird DM, and at least one PC (included as part of the three PCs) equipped with Microsoft Excel, Microsoft Access, Adobe Acrobat, Internet Explorer, and Indiana interChange.
- At least one laser printer
- At least one voice telephone line
- Access to electronic copies of all current versions of users guides, operating procedures manuals, and provider manuals
- Access to electronic copies of manual, bulletin, and banner page templates
- Access to a CD burner
- Access to LAN common drives (I: and L: drives)

The following is additional information about Publications Unit access to information and backups:

- Two electronic copies of all templates on CD-ROM are stored off-site. This CD-ROM is updated and replaced as changes are made to the templates.
- Two electronic copies of all manuals are burned to CD-ROM quarterly and two copies are stored off-site.

In addition, perform daily back-ups of Hummingbird DM. The backup is the first source for all documents and templates in an emergency. If the backup is unable to be retrieved or Hummingbird DM is not able to function for a period, the most recent quarterly manual backups will be used and the template backups will be used.

### ***Third Party Liability***

The Third Party Liability Unit consists of the following employees:

- Three full-time and one part-time health analyst
- Five full-time casualty analyst
- One full-time research/eligibility analyst
- One full-time and one part-time Medicare Buy-In analyst
- One full-time attorney
- One full-time supervisor
- One full-time director

The following are emergency business needs for TPL following a disaster:

- Copier
- Fax machine
- Phones
- Desks
- Paper supplies
- Fifteen PCs connected to Indiana interChange, ICES, On-Demand ( COMMAND), Business Objects, and any other connection currently in place.
- Access to MS Word, Excel, Power Point, and the Internet.

To meet RFP requirements, the following items would need to be established:

- Phone lines for the Health Analysts. The TPL 1-800-457-4510 and the 1-317-488-5046 numbers need to be rerouted or re-established as soon as possible. Phones must be available from 8 a.m. to noon and from 1 p.m. to 5 p.m. Monday through Friday.
- The TPL facsimile line 1-317-488-5217 number needs to be rerouted or re-established as soon as possible.
- An ICES connection must be available for the Buy-In staff and the Research/Eligibility staff.

### ***Office Equipment Recovery***

In the event of a disaster, immediate action must be taken to procure essential office equipment as quickly as possible. EDS facilities in Indianapolis currently occupied by the Indiana Solution Centre

(ICS) will be used as a temporary Disaster Recovery alternate work site, and office equipment may be installed at those ISC sites.

To recover the Indiana Title XIX office equipment, including personal computers, servers, printers, and other miscellaneous office equipment, refer to the *LAN/WAN/CAN Manual*.

The plan is currently stored in a permanent box at the following offsite location:

The documentation listed above contains key contact information within EDS Client Services Group (CSG) and EDS Global Purchasing (PUR). The documents outlines procedures to replace computers, servers, printers, and other miscellaneous office equipment required to restore essential services.

## Section 4: Resumption of Normal Business

---

### Overview

When the Disaster Recovery Phase is complete and essential, services have been restored, the Business Continuity Plan continues with an effort to resume normal business functionality. For this phase of the recovery effort, it is assumed that a suitable permanent work location has been obtained and all necessary equipment and services are available. The goal of this phase of the *EDS Indiana Title XIX Business Continuity Plan* is to complete the recovery process.

### Operating Environment

#### UNIX

When permanent facilities and equipment has been obtained, the UNIX environment will be restored to normal business operations using backup tapes in conjunction with system restore documentation. Full backups of the Sun UNIX processing environment and system restore documentation are currently stored at:

**Iron Mountain  
1165 Girls School Road  
Indianapolis, IN 46231**

The Disaster Recovery documentation for the Sun UNIX environment is insyscfg.xls. This document will have the current equipment and software listed, and procedures to restore data and bring all the equipment back online. The documentation is offsite in a permanent box at the Iron Mountain location listed above.

### Local Area Network

To restore the Local Area Network, including all security files and controls, perform the following actions.

1. Restore servers:

- Obtain servers
- Restore the workgroup servers in the following order:
  - Domain Controller(s)
  - Thin Client Server
  - Application Image Server
  - Document Management Server
  - Imaging Servers
  - All Web Servers

*See Restoring The OS in the Backup/Restore section of the Infrastructure Manual.*

2. Restore connectivity:

- Obtain network hardware

- Establish local area service
- Establish EDSLINK connectivity
- Establish foreign network connectivity

*Note: See Restoring Connectivity in the Infrastructure Manual.*

### 3. Configure and Deploy PCs:

- Obtain PC hardware
- Configure for user environment

*Note: See Desktop Configuration in the Infrastructure Manual.*

## Database Administration

The Oracle RDBMS application resides on DSIBSUN0 (all test databases, all model office databases, and change management), DSIBSUN1 (claim engine and autosys), DSIBSUN2 (production interChange DB, Document Management, and Claims Imaging), and DSIBSUN3 (history, MAR, business objects, and DSS).

## System Overview

This plan covers the recovery of the test, model office, and production DBMS (Oracle) software and data located on DSIBSUN0, DSIBSUN1, DSIBSUN2, and DSIBSUN3.

Recovery includes the test, model office, and production databases.

Recovery and restoration of all DBMS systems is completed at the local site when it is re-established.

### Sizing Requirements

#### DSIBSUN0

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*
- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*

#### Test DSIBSUN0 Databases

- INAIMT1 – 1.4 GB Indiana interChange On-line
- INCEAT1 – 2.1 GB Claim Engine
- INDOCT1 – 831 MB Document Management System and Claims Imaging
- INHIST1 – 1.9 GB History
- INMART1 – 925 MB MAR
- INDSST1 – 915 MB DSS
- INPWBT1 – 2 GB Project Workbook

**DSIBSUN0 Model Office**

- INAIMM1 – 12.7 GB Indiana interChange On-line
- INCEAM1 – 2.1 GB Claim Engine
- INHISM1 – 1.2 GB History
- INDSSM1 – 8.5 GB DSS
- INMARM1 – 7.7 GB MAR
- The SUN0 server runs the test and model office environments as well as the document management and change control databases.

**DSIBSUN0 Other**

- INADMP1 – 1.6 GB Change Management
- MCAIMT1 – 2.5 GB Old Maxi-Care Test Database
- Two Log Files – 1GB each
- Checkpoint Space – 35 GB

**DSIBSUN1**

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*
- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*
- The SUN1 server runs the claim engine and the autosys scheduling software. The POS claims also process on this server.

**DSIBSUN1 Production Databases**

- INCEAP1 – 4.2 GB Claim Engine
- INJOBP1 – 735 MB Autosys Scheduler
- Two Log Files – 1GB each
- Checkpoint Space – 35 GB

**DSIBSUN2**

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*
- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*. The SUN2 server runs the Indiana interChange online database, the Document Management, and Imaging database. A backup claim engine resides on this server. The flat history files are also stored on SUN2. The history files are used during the batch cycles.

**DSIBSUN2 Production Databases**

- INAIMP1 – 181 GB Indiana interChange On-line

- INDOCP1 – 1.2 GB Document Management and Claims Imaging
- Two Log Files – 1GB each
- Checkpoint Space – 35 GB

**DSIBSUN3**

- CPU license required – See Systems Administrator's ADRP
- Size of CPU required – See Systems Administrator's ADRP
- Minimum Memory Requirements – See Systems Administrator's ADRP
- Disk Space for Application – See Systems Administrator's ADRP
- The SUN3 server houses the Decision Support System (DSS), Business Objects, Management and Administrative Reporting (MAR), and history databases.

**DSIBSUN3 Production Databases**

- INHISP1 – 414 GB History
- INDSSP1 – 55 GB DSS
- INDSSP2 – 290 GB History
- INMARP1 – 56 GB MAR
- Two Log Files – 1GB each
- Checkpoint Space – 35 GB

**DSIBSUNB**

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*
- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*
- The SUNB server houses the Production and Model Translator databases.

**DSIBSUNB Production Databases**

- INECGP2 – 6 GB Production Translator
- INECGA2 – 6 GB Model Translator
- Two Log Files – 1 GB each
- Checkpoint Space – 35 GB

**DSIB3**

- CPU license required – See *Systems Administrator's ADRP*
- Size of CPU required – See *Systems Administrator's ADRP*
- Minimum Memory Requirements – See *Systems Administrator's ADRP*
- Disk Space for Application – See *Systems Administrator's ADRP*
- The DSIB3 server houses the Production Project Workbook and the Model MAR databases.

**DSIB3 Production Databases**

- INPWBP! – 4 GB Production Translator
- INMARM2 – 3 GB Model MAR
- Two Log Files – 1 GB each
- Checkpoint Space – 35 GB

*Note: SUN0, SUN1, SUN2, and SUN3 run the Solaris 2.6 operating system. The Oracle database is version 8.0.5. SUNB runs Solaris 8 operating system. The Oracle database is version 8.1.7.4. DSIB3 runs Solaris 9 operation system. The Oracle database is version 9.0.*

## Cycle Recovery Process

To recover each database, complete the following steps. Repeat these steps for each database restoration.

*Note: Refer to the DBA Manual in the Document-Prod library in INDOCP1 for “how to” specifics.*

Environment variables required for production—defined by login file `/home/oracle/.profile`, `.kshrc`):

1. Verify recovery of the Solaris 2.6 platform (See *Systems Administrator's ADRP*).
2. Verify that the Legato Networker utility and the current Legato indexes have been restored.
3. Verify recovery of the password and group files (both NIS and local). Verify that Oracle and DSIBDBA IDs are defined in the local `/etc/passwd` file and the NIS password file.
4. Restore `/opt/???` and `/export/home/oracle` from the UNIX system back-up tapes. This restores only executables and other files, not the DB data files.
5. Determine the exact date and time required for database recovery. Each database can be recovered to a specific point in time as long as all data file locations and archive logs are available at the time the database backup was taken and ending with the required recovery time. This time must be coordinated to allow all database, system, and application files to be restored to the same point in time.
6. Restore all database files from the most recent back-up tapes. The back up used must have been complete before the determined date and time. If the backup was still running at that time, use the back-up tapes from a previous backup. If the back-ups were taken while the database was up, back-up tapes and archive tapes are needed. If the back-ups were taken while the database was down, all tapes must be from the same backup.
7. Restore the database data files, archive logs, and control files. The log file that was current while the backup was being taken must be restored.
8. Install current version of Oracle software.
9. Verify all database row device locations were created at the correct size. Create directory structures for each database.
10. Verify all startup parameters are set up correctly in the `init.ora` files for each database and verify all database create scripts, and run to create new databases.
11. Restore all data files, redo logs, and control files to the correct locations. Begin individual database recovery processes.
12. Roll forward using archive logs to a specific point in time.

13. If necessary, change global netutil entries to correspond to the new database server. Use the *\$II\_SYSTEM/oracle/bin/netutil* utility.
14. Verify the creation of the database—run some test queries, run a batch job script to test remote access, run the UNIX online executable, run a GQL query if a configured PC is available.

## Telecommunications

In the event of a disaster, immediate action must be taken to resume telecommunication services as quickly as possible. EDS facilities in Indianapolis currently occupied by the Indiana Solution Centre will be used as a

Temporary Disaster Recovery alternate work site. Voice and data communications for Indiana Title XIX personnel will have to be established at these sites.

To recover the Indiana Title XIX voice and data communications environment in case of a partial or total disaster, see the following documentation:

- *Voice Network Recovery Plan*
- *Data/Network/Circuit Recovery Plan*

These plans are currently stored in a permanent box at the following offsite location:

**Iron Mountain  
1165 Girls School Road  
Indianapolis, IN 46231**

The documentation listed above contains key contact information, voice and data circuit information, and a list of critical phone numbers and T1 configuration information. The documents also outline procedures to restore data and voice communication and bring all required equipment back online.

## Applications

Restoration of the EDS Indiana Title XIX application environment requires the ability to support all business and system functionality with a full EDS staff. In addition to direct technical support of the Indiana interChange application, the recovery of Finance, Provider Enrollment and Resolutions and Adjustments are required in order to provide full functionality.

### ***Indiana interChange Support***

To support the Indiana interChange system, a normal EDS office environment must be provided for all personnel at the permanent site. These facilities must contain PCs capable of accessing EDSNET and the public Internet, in addition to normal office equipment (such as, desks, chairs, phones, copiers, fax machines, and so forth). EDS support personnel must have normal access to the Indiana interChange system to support system functionality, verify processing results, respond to client inquiries, and make any modifications or corrections that are necessary for normal business operations. In addition, the following software and/or hardware must be installed on the indicated number of PCs.

- Powerbuilder v 7.03 – 6 PCs
- LBMS client – 18 PCs
- Business Objects – 6 PCs

- Reflections – 18 PCs
- 56K V92 Modem – 1 PC

## **Finance**

The Finance Unit consists of ten full time employees that perform the following tasks:

- MAR and CMS 64 Reporting
- Cash control
- Daily provider payment
- Document expenditures
- Daily funding of Medicaid
- Bank reconciliation and tax assessment reconciliation
- Tax assessments
- Expenditures
- Accounts receivables
- Repayment agreements
- Daily balancing and MAR reporting
- Premium vendor services

These tasks fall within the critical path for the processing and payment of claims, and are therefore vital to this account. EDS obtains funds from the State daily to reimburse for Medicaid claims paid that day. It is required that these funds reach a zero balance each day, and failure to do so can jeopardize the entire claims payment process. EDS also performs premium vendor services for CHIP and MEDWORKS members and must be able to send invoices and collect premium payments daily. For this reason, it is critical that these ten performers regain the ability to perform duties as quickly as possible after a disaster.

On-going business needs for Finance following a disaster:

- Ten PCs with EDSNET access to the Indiana interChange system, the Internet, On-Demand, IndianaAIM, DSS, Business Objects, Fifth Third Direct, and one PC must have access to MAR.
- Ten desks
- Ten phones
- One fax machine
- One copier
- Standard office supplies

## **Provider Enrollment**

The Provider Enrollment Unit performs most of its functions within the Indiana interChange system. The unit is unable to operate without access to interChange. In the event of a major business interruption, the Provider Enrollment Unit would become operational when interChange access is restored. This includes the hardware and linkage necessary to operate in the system. The provider enrollment unit works closely with several other units on the account, including Managed Care,

Operations, Finance, and Claims. These units would need to be operational as well for Provider Enrollment to operate normally. The unit's quality analyst produces reports for the OMPP, on quality outcomes. As noted above, most of these reports rely on information contained in Indiana interChange.

On-going business needs for Provider Enrollment following a disaster:

- Access to interChange
- Access to Business Objects
- Access to MiniTab
- Access to Manchester software for the financial analyst
- Access to Document Tracking System (DTS)
- File cabinets
- One printer
- Bookcases
- Fax machine
- Eleven PCs
- Eleven or fewer telephones
- Eleven chairs and work surfaces
- Access to the H drive and the I drive
- Microsoft Office tools, including Access, Word, Excel, and PowerPoint
- Access to DSS
- Access to COMMAND, an On-Demand information storage program
- Adobe Acrobat
- Internet Explorer
- EDSNET
- SAP

### ***Resolutions and Adjustments***

The following lists identify requirements for the permanent business facility.

On-going business needs for Resolutions following a disaster:

- Back up data in Indiana interChange in order to process claims.
- Five PCs
- Printers
- *Claims Resolution Manual*
- Calculators
- Pens
- CRLD backup for reporting

- Back up reports and logs used for daily reporting
- Copies of *Resolutions Operating Procedures Manual*

On-going business needs for Adjustments following a disaster:

- Back up data in Indiana interChange to process Adjustments
- CRLD backup for reporting
- Back up reports and logs used for daily reporting
- Four PCs
- Printers
- Phones
- Calculators
- Pens
- Forms needed to process adjustments
- Copies of *Adjustments Operating Procedures Manual*
- Cabinets to store work

## Manual Processing

Manual Processing at the EDS Indiana Title XIX account is a critical business function. The ability to process Medicaid paper claims timely is required by the contract with the client. A high priority must be assigned this functional area while resuming normal business operations. Manual processing requirements may be divided into Claims and Data Entry.

### **Claims**

The following are on-going business needs for Claims following a disaster:

- All incoming P.O. Box mail must be delivered to the permanent work location.
- A standard office environment is necessary for the team.
- Specific office supplies required include mail sorters, rubber bands, correction tape, highlighters, pens, pencils, letter openers, cabinets, tape, carts, staple pullers, rubber fingers, and rubber gloves.
- Other essential supplies include a letter opening machine, microfilm machines, supplies for microfilm machine, PCs, printer, copier, microfilm, folders, Indiana interchange, and RTP Access data base.
- A copy of the Claims Unit Training Manual must be available.
- A copy of all logs and reports used daily (batch header sheets, batch activation log sheets, microfilming process forms, production reports, production sheets, quality reports, quality sheets, status report, CPC 4, CPC 5, CPC 49, and CPC 16) must be provided.
- Shelving must be available in order to keep all incoming claims for 90 days.
- Quality information for RFP requirements must be collected.
- All copies of claims on microfilm that have not been shipped to warehouse must be moved to the permanent work location.

## **Data Entry**

The Data Entry unit is part of the Claims department and is responsible for the correct entry of all manually processed claim data into IndianaAIM.

On going business needs for Data Entry following a disaster:

- One supervisor
- Twenty-four employees
- Back up Viking system
- Twenty-four terminals
- Data Entry training manual
- System and forms to do quality check in order to meet RFP requirements
- Shelves
- Balance log
- One PC and Microsoft excel
- Twenty-six chairs
- Twenty-six desks
- Production sheets to record batches completed
- Calculator
- Files on employees

## **Output Processing**

The follow are the requirements of the Computer Operations. The Computer Operations Unit is a critical part of the Medicaid essential services, and must be restored as quickly as possible at the permanent location.

### ***SunPrint Server (199.42.137.71)***

Hardware	Sun7 Sparc 10: This unit is back up using the Sun Jukebox DAT tapes that the rest of the Sun Unix boxes are on. Same recovery plan as those boxes. Main software needing restored is listed below.
Software	<ul style="list-style-type: none"> <li>• Solaris 6.2</li> <li>• LP Plus 3.12</li> </ul>

### ***Xerox Elixir Forms PC***

Hardware	<ul style="list-style-type: none"> <li>• Standard Intel Pentium based PC</li> </ul>
Software	<ul style="list-style-type: none"> <li>• Standard image of the Windows 2000 environment.</li> <li>• Office Professional</li> <li>• Paint Shop Professional</li> <li>• Reflections VT200 sessions</li> </ul>

- Elixir desktop with forms, fonts, graphics options loaded
- Elixir print driver converts Windows Documents to Xerox Forms

### ***Xerox Dig path PC/Scanner Station (199.42.136.16)***

#### **Hardware**

- Intel-Based PC with 256+mb of memory
- Three drive partitions
- 5.2GB Optical Worm drive
- 100 MB Nic
- Xerox DigiPath Scanner, UW7A-00651

#### **Software**

- Windows NT 4.0 SP6
- Hummingbird NFS/Telnet/3270 software suite
- Xerox Digipath scanning software version 2.1.2.
- Active Perl 6.2
- ProForm Designer
- Xpert Label 4.15

### ***Blue Server / Streamweaver PC (199.42.136.18)***

#### **Hardware**

- Intel-Based PC with 512+ MB of memory
- 40+ GB of hard drive space
- 100 MB Nic

#### **Software**

- Blue Server Application Server 5.0
- DocSense StreamWeaver software V. 6.0
- DocSense Finalist V. 7.40.00.G
- DocSense Mailer's Choice V. 7.30.GA
- Winzip v. 8.0
- Acrobat - 5.0
- Innoculate Anti-Virus
- PCAnywhere Remote Access Software

### ***Xerox High Speed Printer Hardware***

#### **Xerox LPS controllers**

These controllers hold the logical processing of the printers. All compiled flash form programming exists on these controllers. Xerox will load the base Operating system, to talk to the 4635 printers. All forms, fonts, images, and coding is backed up twice on 3M DC6320 cartridges weekly and one copy is stored offsite. The other cartridge is onsite for quick restore from corruption or unintentional deletions.

Xerox EPS controllers (199.42.136.17, 199.42.136.19) Hardware	<p>The EPS controllers hold all the processing and spool for any jobs received via network printing operations. Most of the jobs are in Postscript format, and some can be received in LCDS Xerox Metacode format. All fonts, forms, and control files are backed up on tape weekly and are available for reload on new printers when they arrive, or at the offsite disaster recovery location.</p>
Software	<ul style="list-style-type: none"> <li>• Sun Blade 1000 dual 700MHZ processor</li> <li>• 100Mb NIC</li> <li>• Sun SLR tape Backup</li> <li>• OS software Version: Solaris 8</li> <li>• Xerox DocUsp Version 6.0.1</li> <li>• Xerox Licenses: <ul style="list-style-type: none"> <li>– VIPP</li> <li>– LCDS Decomposer</li> <li>– LCDS lpr filter</li> <li>– Postscript Interpreter</li> <li>– PCL Interpreter</li> <li>– Xerox Printer Diagnostics</li> </ul> </li> </ul>
Xerox Printer Devices	<p>The Xerox 4635 printers have certain IOT Firmware levels loaded on them to accommodate the various works we do with the Title XIX account and ATD Account. This software will be loaded by the Xerox Field Technicians to any new printers received. Newer DP180 configured with the LPS/EPS controllers.</p>
Miscellaneous Equipment	<ul style="list-style-type: none"> <li>• 100Mb 8-10 port Ethernet hub</li> <li>• 8- 50ft Cat 5 UTP Ethernet cables</li> <li>• Channel Extender (InRange Technologies)</li> <li>• Channel Switch (InRange Technologies)</li> <li>• IDNX Multiplexer Unit (MUX)</li> </ul>
Current Mailroom Post-Print Configuration	<p>The Indiana Title XIX account prints more than 230,000 documents weekly that need to be postmarked and mailed. To efficiently accomplish this task, the account uses two Pitney Bowes Series 8 inserting machines. Each machine is capable of inserting and posting up to 5000 documents per hour. Each machine is configured differently because they were purchased separately over a three-year period. Pitney Bowes software that drives the machines is the main functional difference.</p>

### ***PB Series 8 400R***

Hardware	<ul style="list-style-type: none"> <li>• Pentium level PC</li> <li>• Hi capacity feeder and bed</li> <li>• Dual accumulator units</li> <li>• Folding unit</li> <li>• Transport unit</li> <li>• Three pocket feeders</li> <li>• Enveloper module</li> <li>• Mailpiece re-director table</li> <li>• 2 R150 Series postage meter stations</li> </ul>
----------	---

## Software

- Variable speed envelope output conveyor
- Windows for Workgroups 3.11
- Pitney Bowes ISC2H02 software

**PB Series 8 600R (machine 2)**

## Hardware

- Dell Pentium level PC
- Touch-screen monitor
- Hi capacity feeder and bed
- Dual accumulator units
- Folding unit
- Transport unit
- Ten pocket feeders
- Enveloper module
- Mailpiece re-director table
- Two Output postage meter stations
- Variable speed envelope output conveyor

## Software

- Windows NT 4.0 Embedded Server software
- Pitney Bowes Direct Connect V 1.60.085 D
- Microsoft Access
- MicroTouch Touch-screen enhanced Software

**Paragon Mailing Machine**

- Model # UF60
- Serial # 32468
- Meter Serial # 7039589

**Data-card**

The data-card machine is used to create ID cards for Indiana. Currently, about 8,000 cards are processed each week and are mailed.

## Hardware

- Pentium-based PC
- Data-card 7000 with three modules
- Magstripe, Print, Embosser
- Laser printer
- Ultrapac
- Bridge transport
- Inserter/sealer

## Software

- OS2 Warp
- Datacard 7000 software

## Customers

The Indiana Title XIX print center performs business for several customers that have unique disaster recovery requirements. All customers require recovery of print resources, while some also require inserting. The following are the customer descriptions, disaster requirements, and proposed solutions.

### Print Requirements

- 1.2 million sheets of print per month

### Insert Requirement

- One million sheets inserted, posted, and mailed
- Approximately 350,000 pieces of mail per month

### Expected Recovery Time

- Partial disaster: one week
- Catastrophic disaster: 30 days

Table 4.37 - Required Resources

DC - Divers.	IN Medicaid Cards - 3,000/ctn - 500/box	12186
DC - Divers.	IN Medicaid Card Carriers - 1,500/ctn	70-068-C
DC - ENV	IN Medicaid Envelopes - 9205 permit - 2,500/	101-0002
PAPER	9 1/2 x 11 20Lb 1 part continuous, strip-off perf	2016
ENV - IN6x9.5	6 x 9.5 envelope for RA, PMP, Enrollment	IN6x9
ENV - IN9x12	9 x 12 EOB W/Vert RA's	912EOB-IN
ENV - IN10011	10 x 13 EOB W/Vert - EDS logo (old RA)	1013EOB-IN
ENV	#10 Left Window - EDS	101-0003
ENV - IN10005	#10 Right Window - EDS	757031
ENV	#10 Double Window Env (plain datacard)	101-0001
ENV - MISC000	11 1/2 x 14 1/2 No Window - EDS	761132

### Planned Print Recovery

In the event of a disaster, the print resources at the Oklahoma Title XIX account can be used until a printer can become functional at local disaster recovery site. All output would be printed, boxed, and sent back to Indiana Title XIX for output processing.

Oklahoma will need to have the following items to be able to perform these tasks:

- Printer controller must have LCDS filter loaded onto the system.
- Printer controller must have LCDS Decomposer installed on the system.
- Printer controller will must have the previous two licenses installed

- Printer controllers will have all the LCDS resource backup tapes to have the most current printer programming loaded on them.

#### **Planned Inserting Recovery**

Oklahoma Title XIX does not currently have the ability to perform back-up inserting for Indiana Title XIX due to incompatibilities in scanner technology. OMR scanners can be upgraded to perform inserting and Indiana Title XIX would be billed for postage charges.

Postmasters will accommodate the 6x9 and #10 envelope insert processing. All mail would then be presorted and mailed according to standards.

Account personnel could hand insert 9x12 flats until a new inserter can be installed.

#### **Planned Datacard Recovery**

Oklahoma Title XIX and Pennsylvania Title XIX currently perform datacard services and are a back up to the Indiana Title XIX account. The datacard files would be FTP'd and inserted at the designated site, until a Datacard machine could be installed in Indiana. Twenty thousand cards will be released to the designated sights upon a two day expectation of the Indiana interChange Disaster recovery system being functional at its alternate location.

Datacard eligibility jobs, *ELGJD041* and *elgjd041.sh*, must be modified with the designated datacard recovery sight's IP address and logon information.

## **Logistical Support**

Logistical Support at the EDS Indiana Title XIX account consists of six areas. Client Services, Electronic Solutions Help Desk, HCBS Waiver and Hospice, Office Equipment Recovery, Managed Care, and Third Party Liability requirements are all listed below. These requirements would have to be met at the new permanent work location to restore a normal business operations environment.

### **Client Services**

The client services director leads four business units within the Client Services department located on the 11<sup>th</sup> floor of 950 North Meridian Street, including Customer Assistance, Written Correspondence, Provider Enrollment, and Provider Representatives.

The four units share some tools, such as a fax machine and a LAN printer/copier with white paper, laminator, 3-hole punch, heavy-duty stapler, LAN I:drive, outlook (e-mail), office supplies, Internet access, and TV/VCR combo. In addition to each unit's individual needs, these shared tools are also necessary for the units to function. The five units also share EDS internal services, such as the courier service to HCE and the OMPP. Each unit has a supervisor...

The following pages of requirements are unit-specific.

#### **Provider Representatives**

The contract requires EDS to retain representatives on staff to visit, educate, and answer questions for providers associated with the Indiana Health Coverage Programs. While the phone staff can answer most questions, some are more complex, or individualized questions, and are referred to the representative for that territory. Representatives work both in and out of the office; have cell phones, laptops, and company vehicles. In the event of a disaster, it would not be likely that all of the aforementioned equipment would be lost.

The following are on-going business needs for Provider Reps following a disaster:

- One supervisor
- Twelve provider reps
- Twelve desks with overheads
- Twelve chairs
- Twelve laptops
- Twelve docking stations
- Twelve laptops and dialup access
- Twelve cell phones
- Rolling briefcases for each representative
- Business cards for each representative
- Ten cars
- Eleven lateral file cabinets
- Three data shows and two screens
- Indiana interChange and On-Demand availability
- Twelve provider manuals
- Twelve desk phones
- Three rolling carts for workshops
- Miscellaneous workshop supplies (such as power cords, provider manual CDs, and so forth)

#### Customer Assistance (Phone staff)

The contract requires EDS to answer provider and member calls for the IHCP within two minutes of calling into the queue between the hours of 8 a.m. and 12 p.m. and 1 p.m. and 5 p.m., Monday through Friday, excluding State holidays. For Premium Vendor Services, the hours are of 8 a.m. and 7 p.m., Monday through Friday, excluding State holidays. The phone staff uses 20 phones with headsets, computers, IndianaAIM, Web interChange, On-Demand, the provider manual, two telephones with taping capabilities, blank tapes, and copies of banner pages and bulletins to perform required duties. In the event of a disaster at 950 N. Meridian Street, the majority of equipment would be lost.

The following are on-going business needs for Customer Assistance following a disaster:

- One supervisor
- Twenty phone staff
- Twenty-one desks, chairs, and PCs
- Twenty-one phones with headsets
- Access to Web interChange and ON-Demand
- Five 800 lines
- Two local lines
- One printer
- Twenty-one provider manuals
- Two telephones with recording capability

**Written  
Correspondence**

The contract requires provider and member written requests for the Indiana Health Coverage Programs responded to within 10 business days of receipt. The written correspondence staff uses five computers, Indiana interChange, On-Demand, the provider manual, and copies of banner pages and bulletins to perform duties. In the event of a disaster at 950 N. Meridian Street, the majority of the equipment would be lost.

The following are on-going business needs for Written Correspondence following a disaster:

- One supervisor
- Four staff
- Five desks, chairs, and PCs
- Five phones
- Indiana interChange and On-Demand availability
- Five provider manuals, bulletins, and banner pages
- Six file cabinets
- One Printer

***Electronic Solutions Help Desk***

The Electronic Solutions Help Desk provides telephone support for the following areas:

- Providers and clearinghouses sending or receiving electronic data
- Providers using the OMNI eligibility system
- Providers using EDS Web interChange
- EDS internal infrastructure helpdesk support

The help desk has a phone system with three separate incoming lines - for ECS support at XXX-XXX-XXXX or toll free XXX-XXX-XXXX, OMNI system support at XXX-XXX-XXXX or XXX-XXX-XXXX, and internal infrastructure support at XXX-XXX-XXXX.

**Physical Set Up**

To establish a permanent location, the following equipment and supplies are necessary to accommodate responses to the provider / vendor community.

- Five support personnel
- One Omni device
- Five desks
- Five chairs
- Five PCs
- Five power surge protectors with multiple plug in capacity
- Two five drawer filing cabinets
- Five phones with three separate lines each
- General office supplies – paper, pens, stapler, paper clips, file folders, hanging files, Julian calendar
- Fax machine

- Printer connected to LAN

**Communication Requirements**

- Connection to Sun 5
- Connection to Sun 6
- Connection to Sun 0
- Connection to Sun B
- Connection to Sun 2
- Connection to Internet – for Web interChange
- Access to LAN
- Access to Outlook

***Home and Community Based Services Waiver***

The Home and Community Based Service (HCBS) waiver consists of 13 full time employees that perform the following tasks:

- One Clerical Support
- One Supervisor
- Eight HCBS Waiver Review Analysts
- Two Recoupment Analysts
- One Waiver Specialist

This response plan is based on the contract in year 2002. The Waiver Support position tasks fall within the critical path for the notification for scheduling all waiver reviews and the processing and payment of recoupments, and are therefore vital to continuing meeting RFP contractual obligations. The provider notification for both waiver and hospice reviews is required two weeks before the scheduled review. It is critical that this one individual performer regain the ability to perform their duties as quickly as possible after a disaster. This department's requirement for the Disaster Recovery Phase of the Business Continuity Plan is to have a standard office environment setup for one individual during the first week after the disaster.

The following are on-going business needs for HCBS following a disaster:

- One PC with EDSNET access to the Indiana interChange SUR subsystem, Insite, and the ability to access the public internet
- Desk
- Phone
- Fax
- Copier
- Office supplies

The Indiana interChange SUR subsystem is critical for providing HCBS waiver teams the claims history reports for completing the contract-required reviews. There will be a CD file of all Waiver forms housed off-site, with a copy of the response and recovery plan. The 10 review analysts, the supervisor, and waiver specialist would need to regain the ability to perform their duties two weeks

post disaster. The setup would include 10 laptop computers, and six printers, four docking stations, and other office equipment considered normal in a standard business environment (desk, phone, fax, copier, office supplies, and so forth). Review teams are in the office one week per month. If the review teams are not in the office at the time of the disaster, this equipment would not be needed immediately. The review teams would need access to the Unit L: drive with files restored, EDSNET, Indiana interChange, Insite database, and the ability to access the public Internet. Additionally, the two waiver recoupment analysts would need PCs with access to Indiana interChange within two weeks post disaster. This will enable recoupements identified during the audits to be performed.

## **Long Term Care**

The Long Term Care Unit consists of 16 full-time employees:

- One director
- One supervisor
- Twelve Long Term Care Review Analysts
- One Statistical analyst
- One Clerical Support Staff

This response plan is based on the contract in year 2004. The LTC unit's responsibilities of auditing LTC facilities, and the compilation and reporting of data obtained during these audits, is a condition of meeting RFP contractual obligations. It is critical that one individual performer regain the ability to perform duties as quickly as possible after a disaster. This department's requirement for the Disaster Recovery Phase of the Business Continuity Plans is to have a standard office environment setup for one individual during the first week after the disaster.

The following are emergency business needs for LTC following disaster:

- One PC with access to IndianaAim and MAR
- Desk
- Phone
- Fax
- Copier
- Office Supplies

There will be a CD file of all LTC forms housed off-site, with a copy of the response and recovery plan. The twelve review analysts would need to regain the ability to perform their duties two weeks post disaster. The setup would include thirteen laptop computers, which each analyst currently has in their possession, six printers, four docking stations, and other office equipment found in a standard business environment, such as desks, phones, fax machine, copier, and office supplies. Review teams are in the office throughout the week, and this equipment would be needed as soon as possible. The review teams would need access to the L Drive with files restored, EDSNET, IndianaAim, and the public internet. Additionally, the two waiver recoupment analysts would need PCs with access to Indiana interChange within two weeks post disaster. This will enable recoupements identified during the audits to be performed.

## **Managed Care**

The Managed Care Unit performs most of its functions within the interChange system. The unit is unable to operate without access to interChange. In the event of a major business interruption, the managed care team would become operational when interChange access is restored. This includes the hardware and linkage necessary to operate in the system. The Managed Care Unit works closely with several other units on the account, including Provider Enrollment, Operations, and Claims. These units would need to be operational for Managed Care to operate normally. In addition, Provider Enrollment houses managed care enrollment paperwork. The majority of documentation could be lost or destroyed in a major disaster.

The following are on-going business needs for Managed Care following a disaster:

- Access to interChange
- Access to Business Objects, MiniTab, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, the H drive, and the I drive
- Access to Document Tracking System (DTS)
- Seven PCs
- Seven or fewer, telephones
- Connection to a printer
- Seven chairs and work surfaces
- File cabinets for paper documentation
- Access to CRLD
- Access to Adobe Acrobat
- Access to Internet access
- Access to EDSNET
- Access to SAP

## **Publications**

The contract requires EDS to maintain operating procedure manuals, provider manuals, user's guides, to produce periodic bulletins, and weekly banner pages to communicate with providers (and members) enrolled in the IHCP.

The Publications Unit uses telephones, PCs, and reference materials (including dictionaries, thesaurus', style guides, technical writing guides, and other reference manuals) to verify information used in the documents being written, edited, or reviewed. The Publications Unit uses Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Outlook, Microsoft Access, Adobe Acrobat, Internet Explorer, Indiana interChange, and Hummingbird DM.

The following are emergency business needs for Publications following a disaster:

- One supervisor
- Four employees
- Five desks
- Five chairs
- Five PCs, equipped with Microsoft Word, Microsoft Outlook, and Hummingbird DM, and at least one PC (included as part of the three PCs) equipped with Microsoft Excel, Microsoft Access, Adobe Acrobat, Internet Explorer, and Indiana interChange.
- At least one laser printer

- At least one voice telephone line
- Access to electronic copies of all current versions of users guides, operating procedures manuals, and provider manuals
- Access to electronic copies of manual, bulletin, and banner page templates
- Access to a CD burner
- Access to LAN common drives (I: and L: drives)

The following is additional information about Publications Unit access to information and backups:

- Two electronic copies of all templates on CD-ROM are stored off-site. This CD-ROM is updated and replaced as changes are made to the templates.
- Two electronic copies of all manuals are burned to CD-ROM quarterly and two copies are stored off-site.

In addition, perform daily back-ups of Hummingbird DM. The backup is the first source for all documents and templates in an emergency. If the backup is unable to be retrieved or Hummingbird DM is not able to function for a period, the most recent quarterly manual backups will be used and the template backups will be used.

### ***Third Party Liability***

The TPL Unit consists of the following employees:

- Three full-time and one part-time health analyst
- Five full-time casualty analyst
- One full-time and one part-time Medicare Buy-In analyst
- One full-time Research/Eligibility analyst
- One full-time attorney
- One full-time supervisor
- One full-time director

The following are on-going business needs for TPL following disaster:

- Copier
- Fax machine
- Fifteen phones
- Fifteen desks
- Paper supplies
- Fifteen PCs connected to Indiana interChange, ICES, On-Demand (COMMAND), Business Objects, and any other connection currently in place.
- Access to Microsoft Word, Excel, PowerPoint, and the Internet.

To meet RFP requirements the following items would need to be established:

- Phone lines for the Health Analyst. The TPL XXX-XXX-XXXX and XXX-XXX-XXXX numbers need to be rerouted or re-established as soon as possible.

- An ICES connection must be available for the Buy-In and Research/Eligibility staff.

### **Office Equipment Recovery**

During the recovery from a disaster, action must be taken to procure essential office equipment to restore a normal operating environment. The following documentation assumes that a permanent facility has been located, and the EDS Indiana Title XIX account will obtain the necessary office equipment to furnish those facilities as part of the recovery effort.

To recover the Indiana Title XIX office equipment, including personal computers, servers, printers, and other miscellaneous office equipment, see the *LAN/WAN/CAN Manual*.

This plan is currently stored in a permanent box at the following offsite location:

**Iron Mountain  
1165 Girls School Road  
Indianapolis, IN 46231**

The documentation listed above contains key contact information within EDS Client Services Group (CSG) and EDS Global Purchasing (PUR). The documents also outline procedures to replace computers, servers, printers, and other miscellaneous office equipment required to restore a normal business operations environment.

## **Section 5: Business Continuity Plan Maintenance**

---

### **Distribution of the Plan**

Copies of this *EDS Indiana Title XIX Business Continuity Plan* should be maintained in the following locations:

- EDS/Indiana Title XIX online document turnover directory
- Members of the Initial Response Team should have a copy at their residence. Initial Response Team members are listed in *Section 6 – Contacts*.
- Members of the Crisis Management Team should have a copy at their residence. Crisis Management Team members are listed in *Section 6 – Contacts*.
- Members of each of the Contingency Management Teams should have a copy at their residence. Contingency Management Teams and their respective members are listed in *Section 6 – Contacts*.

### **Updating the Plan**

The following sections of the *EDS Indiana Title XIX Business Continuity Plan* contain information that is relatively stable, and should only need a cursory annual review.

- *Section 1: Business Continuity Plan Overview*
- *Section 2: Crisis Management*
- *Section 5: Business Continuity Plan Maintenance*
- *Section 7: Forms and Tools*

The following sections of the *EDS Indiana Title XIX Business Continuity Plan* contain information that is subject to change, and should be reviewed in detail and updated on an annual basis.

- *Section 3: Disaster Recovery*
- *Section 4: Resumption of Normal Business*
- *Section 6: Contacts*

### **Approval of the Plan**

Changes to the *EDS Indiana Title XIX Business Continuity Plan* should be coordinated through the Business Continuity Plan Project Leader. When revised, the new Business Continuity Plan should be reviewed and approved by a member of the local Crisis Management Team. This process should take place annually, and the revised Business Continuity Plan should be distributed as described above.

### **Testing the Plan**

The *EDS Indiana Title XIX Business Continuity Plan* should be tested after every significant update or revision. The recommended frequency for updating and testing is on an annual basis. The actual frequency of these activities will be at the discretion of the local EDS account management team.

To test the *EDS Indiana Title XIX Business Continuity Plan*, a Disaster Recovery Test Project Leader should be identified. That individual will have the responsibility to do the following:

- Make all arrangements required to conduct a Disaster Recovery Test. This may include, but is not limited to, the following:
  - Obtain management commitment for required manpower resources at the EDS Indiana Title XIX account.
  - Reserve time, equipment, and other resources required at the recovery site.
  - Define a hypothetical disaster scenario that would result in a significant service interruption if it actually took place. Document this disaster scenario in preparation for a test.
  - Choose a date and time for the hypothetical disaster scenario to occur. At the appointed time, inform a member of the Initial Response Team of the disaster.
- Observe and document the efforts of the Response Team, as well as the Local Crisis Management team and the appropriate Contingency Management Team(s) as they respond to the simulated disaster. Use the *Test Results Report* form found in *Section 7: Forms and Tools* to document the outcome.

## Section 6: Contacts

---

### Initial Response Team

One or more members of this group should be contacted immediately when any potential disaster situation exists. These individuals will investigate the situation and determine whether or not a disaster should be declared.

Table 6.1 – Initial Response Team Contact Information

Name	Work Phone	Home Phone	Other Contact Method

### Crisis Management Team

When a disaster has been declared, this group will be responsible for the direction and oversight of all efforts associated with the recovery process. This group will be responsible for obtaining the necessary resources and providing required status reports, including the Response To Operational Problems (RTOP) process.

Table 6.2 – Crisis Management Team Contact Information

Name	Work Phone	Home Phone	Other Contact Method

## EDS Corporate Crisis Management Office

The Local Crisis Management Team will contact the EDS Corporate Crisis Management Office in the event of a disaster. The EDS Corporate Crisis Management Office will provide corporate assistance and act as a liaison to other corporate support groups.

Table 6.3 – EDS Corporate Crisis Management Office

Name	Phone Number

## Contingency Management Teams

These teams will engage in the disaster recovery process if the Local Crisis Management Team believes their participation is necessary. Additional resources may also be engaged at the discretion of the Local Crisis Management Team.

Table 6.4 – Operating Environment Contingency Management Team

Name	Work Phone	Home Phone	Other Contact Method

Table 6.5 – Telecommunications Contingency Management Team

Name	Work Phone	Home Phone	Other Contact Method

Table 6.6 – Applications Contingency Management Team

Name	Work Phone	Home Phone	Other Contact Method

Table 6.7 – Manual Processing Contingency Management Team

Name	Work Phone	Home Phone	Other Contact Method

Table 6.8 – Output Processing Contingency Management Team

Name	Work Phone	Home Phone	Other Contact Method

Table 6.9 – Logistical Support

Name	Work Phone	Home Phone	Other Contact Method

## EDS Support Organizations

Table 6.10 – EDS Support Organizations List

Name	Address	Phone

## EDS Security

Table 6.11 – EDS Security

Name	Address	Phone

## Building Security and Maintenance

Table 6.12 – Building Security and Maintenance

Name	Address	Phone

## Local Authorities and Emergency Services

Table 6.13 – Local Authorities and Emergency Services

Name	Address	Phone
Indiana Emergency Management	302 W. Washington St.	(317) 232-3980
<b>Indianapolis Fire Department</b>		
Administration	555 N. New Jersey	(317) 327-6041
Fire Prevention	620 N. Sherman Dr.	(317) 327-6006
<b>Indiana Public Works</b>	402 W. Washington	(317) 232-3000
Environmental	100 N. Senate Ave.	(317) 232-8603 1-800-451-6027
POLICE/FIRE/EMS Emergency		911
Indianapolis Police General Information	47 S. State Ave.	(317) 327-3811
Fraud Investigations		(317) 327-3568
Indianapolis Fire Dept./EMS General Information		(317) 327-6041
Indianapolis Emergency Management	47 S. State Ave	(317) 327-3900
Indiana State Fire Marshal		(317) 232-2222
Indiana State Police– District 52		(317) 232-8250
Disaster Response and Recovery		(800) 669-7362
Indiana Dept. of Environment Management		1– (888) 233-7745
Environmental Protection Agency	77 W. Jackson Blvd. Chicago, IL 60604	(800) 621-8431

Table 6.13 – Local Authorities and Emergency Services

Name	Address	Phone
Federal Information Center		(800) 688-9889
Hazardous Materials Information Line		(800) 467-4922
National Response Center		(800) 424-8802
Spills (24 hours a day)		
National Weather Service Administration	6900 West Hanna Ave Indianapolis, IN 46241	(317) 856-0360
Indianapolis and Vicinity Forecast (24 hours a day)	Listen to KC74 162.55	(317) 635-5959

## Public Utilities

Table 6.14 – Public Utilities

Name	Address	Phone
REI Investment Inc. (Utilities are handled by landlord).	11711 N. Meridian Carmel, IN 46032	(317) 573-6050
Indianapolis Power & Light	One Monument Circle Indianapolis	(317) 261-8222 Emergencies (317) 261-8111
Indianapolis Water Company	1220 Waterway Blvd. Indianapolis	(317) 639-1501 Emergencies (317) 631-1431
Main Post Office Information Box Rent and Meter Settings Nights, Saturday, Sunday	125 W. South Street	(317) 464-6000 (317) 464-6374 (317) 464-6330
Postal Inspectors	7188 Lakeview Parkway W. Dr. Indianapolis	(317) 328-2500

## Suppliers and Vendors

Table 6.15 – Suppliers and Vendors

Name	Address	Phone

Table 6.15 – Suppliers and Vendors

Name	Address	Phone

## Rental Contacts

Table 6.16 – Rental Contacts

Equipment	Company	Address	Phone

## Mailing Service Contacts

Table 6.17 – Mailing Service Contacts

Company	Address	Phone

## Lodging Contacts

Table 6.18 – Lodging Contacts

Company	Address	Phone

## Medical Contacts

Table 6.19 – Medical Contacts

Company	Address	Phone

## Transportation Contacts

Table 6.20 – Transportation Contacts

Equipment	Company	Address	Phone

## Communications Contacts

Table 6.21 – Communications Contacts

Use	Phone Number/Circuit ID	Vendor	Remarks

## Document Control Contacts

Table 6.22 – Document Control Contacts

Contact	Phone

## Section 7: Forms and Tools

---

### Description of Contents

The following lists the forms and tools found in this section:

- Business Continuity Self Assessment
- Business Area Risk Assessment
- Business Impact Matrix
- Critical Business Process worksheet
- Initial Assessment Checklist
- Applications Assessment
- Manual Processing Assessment
- Operating Environment Assessment
- Output Processing Assessment
- Building Assessment
- Bomb Treat Checklist
- Chemical and Biological Agent Procedures
- Threat and Vulnerability Worksheet
- Community Resources Worksheet
- Customer Meeting Topics
- Crisis Management Plan Outline
- Employee Communication Procedures
- Employee Contact Sheet
- Employee Recovery Needs Assessment
- Team Safety Assessment
- Training Topics
- Problem Log
- Public Relations Guidelines
- Recovery Plan Outline
- Recovery Planning Team
- Recovery strategy Meeting Agenda
- Recovery Team Responsibilities
- Service Provider Questions
- Telecommunications Services
- Test Plan – Executive Summary
- Test Results Report

## Business Continuity Self Assessment

To complete this survey, read each question or statement and answer by checking either Yes or No.

Organization \_\_\_\_\_ Evaluator \_\_\_\_\_ Date \_\_\_\_\_

### A. Business Continuity Methodology

1. ☐ Yes ☐ No Do you have a copy of the EDS Business Continuity Policy?
2. ☐ Yes ☐ No Do you annually communicate the EDS Business Continuity Policy to your employees?
3. ☐ Yes ☐ No Have you reviewed the EDS Business Continuity Policy with your customer(s)?
4. ☐ Yes ☐ No Has a business continuity coordinator been identified on your account who is responsible to the account manager?
5. ☐ Yes ☐ No Are you using a standardized methodology to develop and maintain your business continuity plan? (For example, EDS supports a corporate business continuity planning methodology. Many vendor solutions are also available.)
6. ☐ Yes ☐ No Have you developed a list of all the products and services you provide to your customer?
7. ☐ Yes ☐ No Has a risk assessment (risk analysis and business impact analysis) been performed on the products and services provided at each site? (For example, has the impact to your customer and EDS (monetary, personnel, customer satisfaction) been defined if these services are temporarily or permanently unavailable?)
8. ☐ Yes ☐ No Have the recovery requirements been prioritized for the products and services provided?
9. ☐ Yes ☐ No Has your customer reviewed and approved the prioritized list of products and services, the risk assessment, and recovery priorities?
10. ☐ Yes ☐ No Have you developed a comprehensive list of possible disaster scenarios? (For example, have you determined various types of processing losses; such as loss of data entry, the entire processing site, Remote Job Entry sites, the network, the office location, and the phone system?)
11. ☐ Yes ☐ No Have you identified all contractual requirements for recovery of processing, services, and products; or if no formal written contractual requirements exist, have you determined the accepted industry standards that may apply?
12. ☐ Yes ☐ No If required, do you have formal, written approval of the EDS Account Recovery Plan from your customer? (For example, the FFIEC expects each institution to approve EDP recovery plans periodically.)
13. ☐ Yes ☐ No Do you budget for business continuity planning and testing?
14. ☐ Yes ☐ No Are you aware of the EDS Corporate Crisis Management team and the services it can provide?

**B. Business Continuity Audit**

1. ☐ Yes ☐ No Has your recovery plan been reviewed by any auditing group? (Examples may include EDS Corporate Audit, state and federal regulatory examiners, or the customer's EDP audit staff.)
2. ☐ Yes ☐ No Did any of the reviews identify major findings or risks related to the existing recovery plan or emergency procedures?
3. ☐ Yes ☐ No Do you have corrective action initiatives in process (or completed) to resolve each identified audit finding?

**C. Integrated Recovery Plan**

1. ☐ Yes ☐ No Have you identified all the groups that provide services to your account? (For example, account personnel; EDS internal support groups, customer groups, or vendors.)
2. ☐ Yes ☐ No Have you furnished each of your service providers with the customer's documented recovery requirements?
3. ☐ Yes ☐ No Have you documented the relationships existing among your account, your customer, and each of the service providers to clarify the responsibilities of and dependencies between each of the groups?
4. ☐ Yes ☐ No Do you have a written and integrated Account Recovery Plan that includes the following major components:
  - Key customer information
  - Definition of products and services
  - Notification and escalation procedures
  - Summary of service providers and their recovery strategies
  - Relationship between providers and their products and/or services
  - Definition of loss scenarios
  - Critical information inventory
  - Important contacts
  - Detailed Recovery Plan (or Site Recovery Plan)
    - Recovery team assignments
    - Applications
    - Operating Environment
    - Telecommunications
    - Output Processing
    - Manual Processing
    - Administrative Support
  - Recovery schedule with milestones
  - Documented testing strategy
  - Plan maintenance procedures
5. ☐ Yes ☐ No If the Account Recovery Plan is not complete, do you have a schedule for

- completion within the next 12 months?
6. ☐ Yes ☐ No Do you have a written, complete, and approved copy of each service provider's and/or vendor's recovery strategy as it relates to your account?
7. ☐ Yes ☐ No Do you have a current list that includes key contact information and escalation procedures for each customer?
8. ☐ Yes ☐ No Do you have a current list that includes key contact information and escalation procedures for each service provider or vendor?
9. ☐ Yes ☐ No Do you have a current list of other important contacts such as police and fire department, office supply companies, moving and storage companies, hardware and software vendors, utility companies, EDS management or support groups, and local housing?
10. ☐ Yes ☐ No Does your recovery plan track recovery milestones for all account groups and service providers?
11. ☐ Yes ☐ No Have you documented processing priorities to ensure critical applications are recovered completely prior to less critical processing?
12. ☐ Yes ☐ No Does your application recovery strategy use an automated tool to recover all EDS-supported applications? (For example, the EDS Application Disaster Recovery Plan (ADRP) can be used for IPC-based application recovery plans.)
13. ☐ Yes ☐ No Have you defined and documented telecommunications (voice, data, video) recovery requirements with your customer?
14. ☐ Yes ☐ No Does your account have a telecommunications recovery plan to meet customer requirements?
15. ☐ Yes ☐ No Does your account have a documented recovery plan that provides for the backup and relocation of all services performed at the account site location? For example, services may include back office, clerical, billing, and customer service functions.
16. ☐ Yes ☐ No Has your customer provided a copy of his business resumption plan?
17. ☐ Yes ☐ No Has account management, customer management, and major service providers met within the prior twelve months to review the Account Recovery Plan to ensure it meets customer requirements?
18. ☐ Yes ☐ No Do you have written procedures to ensure that the Account Recovery Plan is updated appropriately and reviewed at least quarterly?
19. ☐ Yes ☐ No Is a current copy of the entire Account Recovery Plan stored in a secure but accessible off-site location?
20. ☐ Yes ☐ No Have you appointed a recovery coordinator and organized recovery teams, including account staff and service providers, with specific responsibilities to ensure tasks are understood and completed efficiently and accurately?
21. ☐ Yes ☐ No Have key personnel received training on the Account Recovery Plan?
22. ☐ Yes ☐ No Do key recovery personnel have critical sections of the recovery plan stored

at their residences as well as the office?

23. ☐ Yes ☐ No In the event you cannot return to your original facility, have you documented your requirements for restoration or relocation of the facility? (For example, physical space requirements (including building requirements such as HVAC and power), network requirements, furniture, fixtures, equipment, phone/PBX, or supplies.)
24. ☐ Yes ☐ No Does each of your remote locations have a recovery plan that is complete and integrated with the main processing site plan? (For example, remote locations may include RJE, LAN, data entry, or back office operations.)
25. ☐ Yes ☐ No Do you have a plan to notify your customer of information they will need in the event of a disaster at EDS? (Information may include new customer service phone numbers, new courier delivery locations, or interim manual procedures to replace services that are normally automated.)

#### **D. Critical Data Retention**

1. ☐ Yes ☐ No Has your account completed a Critical Information Inventory to identify the location(s) of information critical to your processing service, your customer's business, and your account's operation? (For example, information may be stored on a mainframe, personal computers, hard copy files, microfiche, or off-site.)
2. ☐ Yes ☐ No Do you have an off-site storage location(s) that is secure, yet accessible, for all critical recovery files, data, supplies, documentation, etc.?
3. ☐ Yes ☐ No Do you have a process (automated or otherwise) to control the movement of all critical recovery files to and from off-site storage? (For example, a tape library system may provide an off-site archival listing.)
4. ☐ Yes ☐ No Does your process prohibit return of key recovery data to the account before replacement files are stored off-site?
5. ☐ Yes ☐ No Do you keep a current listing of all inventory located at the off-site location both at the account site and in off-site storage?
6. ☐ Yes ☐ No Do you perform periodic audits of the off-site inventory to verify all critical information is present and accurate?
7. ☐ Yes ☐ No Do you store critical documentation, forms, procedures, and other key information at an off-site location to ensure its availability during a disaster? (Such documentation may include contract information, invoicing, payroll, or employee information.)
8. ☐ Yes ☐ No Do you store critical data not related to the immediate recovery at an off-site location? (For example, data may include month-end or year-end archival files, regulatory or tax data, or conversion files.)
9. ☐ Yes ☐ No Have you established transportation arrangements for delivery of critical recovery data to the alternate processing location(s) in the event of a disaster?
10. ☐ Yes ☐ No Have you stored proof-of-purchase for client-server and/or LAN software licenses at an off-site location? (For example, you may need a copy of the

license, the original installation diskettes, or copies of the original purchase order to prove insurance claims and facilitate replacement.)

**E. Alternate Process Sites**

1. ☐ Yes ☐ No Have you and/or each of your service providers determined minimum resources (for example, MIPS, DASD, tape, bandwidth) to recover critical processes at the alternate processing site?
2. ☐ Yes ☐ No Has an alternate recovery location been designated (i.e., cold, warm or hot site) that is reasonable, accessible and available to recover your customer's business per their requirements?
3. ☐ Yes ☐ No Do you have a written agreement for an alternate recovery location for each of your processing locations and/or services? (Written agreements can be with another EDS location, a contractual relationship with a recovery site vendor, or a written reciprocal relationship with another local processor.)
4. ☐ Yes ☐ No If this facility is available on a "first come, first served" basis, have you advised your customer of the associated risks?
5. ☐ Yes ☐ No Does your agreement provide reasonable test time (for example, at least 48 hours per year) to allow off-site testing of recovery procedures?
6. ☐ Yes ☐ No Do you have a process defined to negotiate resources available at the alternate site to accommodate changes in the processing requirements?
7. ☐ Yes ☐ No Have you confirmed that resources available at the alternate site are compatible with your normal processing environment? (For example, DASD models or software releases may be incompatible.)
8. ☐ Yes ☐ No Have you made arrangements for account or industry specific equipment that may not be available at a vendor recovery site? (For example, PBX, capture equipment, statement and mail rendering equipment, modems and/or FEPs.)
9. ☐ Yes ☐ No Have you made specific arrangements to re-establish telecommunication links and facilities at the alternate processing locations?
10. ☐ Yes ☐ No Do you maintain a written inventory of communication requirements and, where appropriate, orders to speed re-establishment of the network at both the alternate recovery location and long-term recovery location (if different from the original)?
11. ☐ Yes ☐ No Do you maintain an inventory or have access to backup communications equipment to meet the recovery requirements for critical network operations?
12. ☐ Yes ☐ No Have you made specific arrangements to ensure appropriate physical and data security at the alternate processing location? For example:
  - Some contracts may require EDS personnel (only) to handle data.
  - Confidential data must be deleted from vendor files after a test.
  - Full data security must be in-place during test periods.
  - Magnetic media must be appropriately secure during transportation and while at the alternate processing location.

13. ☐ Yes ☐ No Have you developed procedures for transferring services from the alternate recovery location to the original site or to a newly established location?
14. ☐ Yes ☐ No Have you secured software licenses that allow relocation of vendor software to the alternate site both during a disaster and for recovery tests?
15. ☐ Yes ☐ No Do you have alternate sites for each of your remote locations?
16. ☐ Yes ☐ No Do your remote locations have a means to re-establish communications with the alternate processing site?

**F. Recovery Testing**

1. ☐ Yes ☐ No Have you developed a testing strategy for each of the possible disaster scenarios you developed in the Account Recovery Plan?
2. ☐ Yes ☐ No Have you identified a list of test components that compose the total recovery strategy?
3. ☐ Yes ☐ No Have you tested all components in your testing strategy within the last 12 months?
4. ☐ Yes ☐ No Have you documented the types of tests that you will perform on a pre-determined schedule? (For example, you may do an automated ADRP test of off-site files, an audit of the off-site storage, recovery of the applications at the alternate processing site, recovery of all or part of the telecommunications network, or walk through the account action plan.)
5. ☐ Yes ☐ No Have you identified measurements that ensure your test schedule is appropriate, test results are accurate, test failures are corrected, your recovery plan is cost effective, and your customer accepts the results?
6. ☐ Yes ☐ No Do you routinely include customer participation in your recovery testing to ensure they understand and agree with the risks, the recovery requirements, the recovery milestones, and their responsibilities during an actual recovery?
7. ☐ Yes ☐ No Do you retain a detailed, written log of each completed test with results and action items within the Account Recovery Plan?
8. ☐ Yes ☐ No Have you developed written test scripts, including data input and cycle output review by customer personnel, to ensure completeness and accuracy?
9. ☐ Yes ☐ No Do you appoint a testing drill coordinator and organized test teams, including account staff and service providers, with specific responsibilities to ensure tasks are understood and completed efficiently and accurately?
10. ☐ Yes ☐ No During an off-site processing test, do you establish a testing command center where the ongoing activity of the test can be monitored and coordinated?
11. ☐ Yes ☐ No Do you have comprehensive debriefings after the test to review results, identify corrective action needed, and approve action items?
12. ☐ Yes ☐ No Do you have a procedure to update the Account Recovery Plan and the overall testing plan as a result of findings during a test?

13. ☐ Yes ☐ No Do you communicate test results and plan modifications in an appropriate format to all account staff, providers, customers, and management affected by the test?

**G. Crisis Management Plan (includes emergency procedures)**

1. ☐ Yes ☐ No Have you completed a risk analysis for your account location(s) to identify potential threats (fire, weather, flood, bomb threat, medical, hazardous materials, intrusion, etc.) and made written recommendations on mitigation alternatives?
2. ☐ Yes ☐ No Have you developed a Crisis Management Plan, including emergency procedures? The plan must include the following:
- Posted fire exits and maps
  - Location of emergency supplies
  - Emergency phone numbers
  - Response procedures (based on identified threats)
  - Evacuation procedures (orderly shutdown, retention of critical data, assembly points, post-evacuation procedures)
  - Emergency shift coverage
  - Media relations procedures
  - Emergency communication procedures
3. ☐ Yes ☐ No Are the emergency procedures posted and easily accessible to each employee?
4. ☐ Yes ☐ No Have you coordinated your Crisis Management Plan and emergency procedures with your customer and/or any other group(s) at your site?
5. ☐ Yes ☐ No Does your plan consider the possibility of regional outages where more than your primary site is involved? (For example, regional outages such as severe weather (flood, hurricane, and winter storm) may affect the site, employee residences, transportation, and communications.)
6. ☐ Yes ☐ No Do you have written emergency communications procedures? (These procedures will include distribution lists, voice mail, alternate communications options, such as radio and cellular phone, authorized personnel to release information to the media, and coordination with EDS Public Relations.)
7. ☐ Yes ☐ No Have you installed or implemented emergency equipment, supplies, or procedures? (These may include revised security procedures, installation of fire retardants, posting of escape routes, or the purchase of emergency supplies.)
8. ☐ Yes ☐ No Have you documented prevention measures (implemented or planned) and made this information available to auditors, examiners, and customer management?

9. ☐ Yes ☐ No Have employees been trained in emergency procedures and the use of emergency equipment?
10. ☐ Yes ☐ No Has your account performed an emergency evacuation drill within the last twelve months?
11. ☐ Yes ☐ No Do you have emergency procedures for situations that may affect your employees away from the workplace? (For example, in the event of bad weather, can you communicate with your employees?)

#### **H. Industry-Specific Considerations**

This section includes questions specific to the financial industry. The questions relate to services, regulatory requirements, or industry equipment. Other industries may have different concerns.

1. ☐ Yes ☐ No Have you arranged for recovery of time-sensitive EFT applications such as SWIFT, FEDWIRE, ACH, etc.? (These applications not only have extensive customer risk, they carry certain regulatory requirements.)
2. ☐ Yes ☐ No Have you arranged for recovery of ATM and switch processing? (Special arrangements may include transmission of transaction and positive balance files, special settlement arrangements, limitation of fraud risk, and compliance with special vendor-switch requirements.)
3. ☐ Yes ☐ No If you provide a service that requires industry certification, have you verified that your business continuity plan meets those requirements?
4. ☐ Yes ☐ No Do recovery plans exist for interface to discrete applications (such as trust, payroll, accounting, cash management), which may be processed on mid-range or department-level operating environments?
5. ☐ Yes ☐ No Do you have a recovery plan to restore at least minimal capture operations, and have you made alternate arrangements for Federal Reserve Banks, local clearinghouses and correspondents to accept and deliver cash letters ensuring timely, cost-effective clearing operations?
6. ☐ Yes ☐ No Do you have a recovery plan for back-office services, such as high-volume statement rendering, sort operations, distribution, or couriers?
7. ☐ Yes ☐ No Do you have a recovery plan to restore at least minimal capture operations, and have you made alternate arrangements for Federal Reserve Banks, local clearinghouses and correspondents to accept and deliver cash letters ensuring timely, cost-effective clearing operations?
8. ☐ Yes ☐ No Have you made plans for the protection and recovery of sensitive documents, equipment, and supplies? (For example, negotiable instruments check stock, plastics, embossing equipment, and endorsing equipment.)
9. ☐ Yes ☐ No If you also provide processing or other services to correspondents of your primary customer, have you included their requirements in your planning and have they been informed of your recovery plan?

## Business Area Risk Assessment

Reference	Assessment Question	Current		Is this a threat? (Yes/No/Not Applicable)			Does this require any corrective action? (Yes/No/Not Applicable)			Remarks/Attachments  Note any historical experience with the threat (last occurrence and impact to the site). List actions that should be taken to reduce the likelihood impact or improve response to the threat.  Attach any additional information on this threat.
		Y	N	Y	N	N/A	Y	N	N/A	
<b>Emergency Alarms</b>										
<b>BF1</b>	Are there emergency alarms located within the work area that can warn staff in the event of fire, severe weather, evacuation, etc.?									
<b>BF2</b>	Is everyone in the area trained on the purpose of each alarm and how to respond?									
<b>Emergency Evacuation</b>										
<b>BF3</b>	Are emergency exits clearly marked?									
<b>BF4</b>	Are there multiple exits from the work area?									
<b>BF5</b>	Are emergency exits unobstructed to allow a fast and safe exit from the work area?									
<b>BF6</b>	Are there designated locations or safe areas where employees report in the event of an evacuation?									
<b>BF7</b>	Is there emergency lighting in the work area?									
<b>BF8</b>	Are there individuals in the area that may require assistance due to impairment (hearing, sight, etc)? If yes, are there individuals designated to provide assistance?									
<b>Records Retention/Classification</b>										
<b>BF9</b>	Are there any formal records retention requirements for documents processed in the work area? If yes, are the requirements followed?									
<b>BF10</b>	Are sensitive records stored at a location that is secure and remote from the immediate work area?									
<b>BF10a</b>	Are confidential/sensitive documents shredded prior to discarding?									
<b>BF10b</b>	Is there a document classification system in place?									
<b>BF10c</b>	Are documents properly stored in the work area when staff leaves the area?									

Reference	Assessment Question	Current		Is this a threat? (Yes/No/Not Applicable)			Does this require any corrective action? (Yes/No/Not Applicable)			Remarks/Attachments  Note any historical experience with the threat (last occurrence and impact to the site). List actions that should be taken to reduce the likelihood impact or improve response to the threat.  Attach any additional information on this threat.
		Y	N	Y	N	N/A	Y	N	N/A	
<b>Computer Data</b>										
<b>BF11</b>	If you use computers, i.e., PC, Mini, Mainframe, etc., to perform the process, answer the following questions:									
<b>BF11a</b>	Is your critical computerized data backed up? If yes, are backups stored off-site?									
<b>BF12</b>	Do you know how often the data is backed up, i.e., nightly, weekly, monthly, etc.?									
<b>BF13</b>	Assuming you know when your data is backed up, and you know how old recovered data is backed up, do you have procedures for bringing this information up-to-date?									
<b>Staff</b>										
<b>BF14</b>	Is all skilled staff ever in one location at the same time?									
<b>BF15</b>	Is there an active cross-training program that allows staff to cover for one another in an emergency?									
<b>BF16</b>	Is there an inventory of skills required to perform critical job functions? If yes, who is qualified to perform those functions?									
<b>Notification</b>										
<b>BF17</b>	Is there a list of names, phone numbers and addresses of department employees for emergency purposes? Is this list kept at a secure remote location away from the work area?									
<b>House-Keeping</b>										
<b>BF18</b>	Is the area kept orderly to minimize the risk of fire hazards, trip hazards, and to allow for quick evacuation in an emergency?									
<b>Business Resumption</b>										
<b>BF19</b>	Is there a current business resumption plan that instructs employees to restore critical activities after an emergency and/or disaster?									

Reference	Assessment Question	Current		Is this a threat? (Yes/No/Not Applicable)			Does this require any corrective action? (Yes/No/Not Applicable)			Remarks/Attachments  Note any historical experience with the threat (last occurrence and impact to the site). List actions that should be taken to reduce the likelihood impact or improve response to the threat.  Attach any additional information on this threat.
		Y	N	Y	N	N/A	Y	N	N/A	
<b>Problem Management</b>										
<b>BF20</b>	Are there procedures in place, e.g., escalation, notification, to manage daily problems that may occur, such as, equipment failure, etc.?									
<b>Change Control</b>										
<b>BF21</b>	Are there procedures or processes in place to manage change within the business functions, e.g., computer programs, procedures, processes, personnel, tooling and equipment, etc.?									
<b>Off-Site Storage</b>										
<b>BF22</b>	If off-site storage is in use, please consider the following:									
<b>BF22a</b>	Does the off-site storage facility have heat and smoke detectors?									
<b>BF23</b>	Does the off-site storage facility have a fire suppression system?									
<b>BF24</b>	Is the off-site storage facility restricted from unauthorized access?									
<b>BF25</b>	Is the off-site storage facility at least 2 air miles from the business Process?									
<b>BF26</b>	Is there a list of individuals authorized to retrieve items from off-site storage?									
<b>BF27</b>	Does the list include only current employees?									
<b>BF28</b>	Is the storage facility environmentally compatible for the media being stored, e.g., magnetic tapes, paper, etc.?									
<b>BF29</b>	Has an audit been performed at the off-site location on contents, environment controls, etc.?									
<b>Operating Practices</b>										
<b>BF30</b>	Do all functions or tasks have documented daily procedures?									
<b>BF31</b>	Is all input and output from the process tasks documented?									
<b>BF32</b>	Are all roles and responsibilities of the tasks performed, documented?									

## Business Impact Matrix

### Example:

Risk: Chemical Leak/Spill  
 System/Process/Asset: Data Center Operations Personnel (building evacuation)  
 Probability: High (4)  
 Impact: Catastrophic (4)  
 Score: Probability 4 x Impact 4 = 16 total score

Risk	System/Process/Function/Site/Asset	Probability	Impact	Score (Probability x Impact)

### Key:

Probability of Occurrence	Impact
1 Not Likely	1 Negligible
2 Low	2 Low
3 Medium	3 Medium
4 High	4 Catastrophic

**Business Impact Scale 1-5 (Example)**

Degree of Criticality	Description	Recovery Time Objective (in hours)
5	A failure would result in severe impact to the business. Immediate recovery is required. No down time is allowed. Requires implementing a fully redundant alternative.	0
4	A failure would result in severe impact to the business. Up to 4 hours of down time or inaccessibility can be tolerated. An alternate capability must be functional within a 4-hour time frame.	4
3	A failure would result in impact to the core business. Up to 24 hours of down time or inaccessibility can be tolerated. An acceptable workaround exists that is somewhat complicated and relatively expensive.	24
2	A failure would result in minimal impact to the core business. Up to 72 hours of down time or inaccessibility can be tolerated.	72
1	A failure would result in no measurable impact to the core business. Recovery time objective is greater than 72 hours.	72+

**Dynamic Risk Factor (Sample)**

The Dynamic Risk Factor represents the probability of failure based on things such as the following.  
Risk Key: 1-Low, 2-Medium, 3-High

- Business function interdependencies
- Resource requirements
- Vendor reliability
- Existing risk mitigation
- Existing recovery measures

I have reviewed and agree with the identification and ranking of the critical business processes:

Signed: \_\_\_\_\_

Print: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## Critical Business Process Worksheet

[illegible]

## Initial Assessment Checklist

<input type="checkbox"/> Yes <input type="checkbox"/> No	Do local emergency authorities need to be contacted?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Are there fatalities?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Are there injuries?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Are EDS people unaccounted for?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the situation life threatening?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the team unable to handle the situation?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the facility destroyed?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the facility or area access restricted?
	For how long? _____
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the facility without electrical power?
	For how long? _____
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the facility without water?
	For how long? _____
<input type="checkbox"/> Yes <input type="checkbox"/> No	Can the site be secured?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the facility contaminated?
<input type="checkbox"/> Yes <input type="checkbox"/> No	What type of contamination?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is there extensive fire damage?
	Name the area(s): _____
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is there extensive water damage?
	Name the area(s): _____
<input type="checkbox"/> Yes <input type="checkbox"/> No	Has business "As Usual" been disrupted?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Will there be interference with normal site or business operations?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Does or will the situation result in EDS service disruption?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Will support functions be affected?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Are the initial Response and Unit Crisis Mgmt Team Leaders unaware of the situation?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is furniture unsalvageable?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the hardware extensively damaged?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Are paper documents unsalvageable?
	Describe condition of documents? _____
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is electronic media unsalvageable?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is a professional restoration company needed?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Will the occurrence attract media attention?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Does occurrence need to be reported to local, state, or federal authorities?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Would the occurrence trigger investigations?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is the occurrence a result of EDS actions or lack of action?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Is EDS a victim of external events or forces?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Could the occurrence affect the financial standing of EDS?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Could EDS sales or profits suffer from the occurrence?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Will penalties occur due to the interruption?
<input type="checkbox"/> Yes <input type="checkbox"/> No	Does the Disaster Recovery Plan need to be activated?

## Applications Assessment

1. Have you accounted for any hardware, forms, or supplies that need to be housed at the alternate processing site?
2. Does the hardware at the alternate processing site have sufficient capacity for full recovery?
3. Have you accounted for all software needed to recover your system?
4. For testing purposes, can all licensed software be executed at the alternate processing site?  
If no, please indicate which software cannot be executed?
5. How much disk storage space is needed, and what is the relative processing power required to meet each customer's functional business need?
6. Complete the form below (or attach your own form) to indicate the number of backup generations needed for each application.

Application	# of Backup Generations	Frequency of Backup

7. What application recovery procedures does the customer perform at their work site?

## Manual Processing Assessment

1. If there are any manual processing services supported through a network, please identify the location and service provider below.

Location	Service Provider

2. Describe any special processes not covered in the general questions.

3. Have you accounted for obtaining special supplies and equipment for these processes?

## Operating Environment Assessment

1. If your operating environment supports any channel-extended attached sites, please identify those locations and service providers below.

Location	Service Provider

2. If it is necessary to recover in multiple locations, please list those account names, locations, and contact information below.

Account Name	Location	Contact Name & Phone #

- a. Describe below the situations that cause multiple-site recovery.

3. Identify below or send the rotation schedule of all tapes shipped to an off-site storage facility.

Day of Week	System Cataloged by ...	Shipped Off-Site Time
Monday		
Tuesday		
Wednesday		
Thursday		
Friday		
Saturday		
Sunday		

- a. Who is responsible for the physical relocation of backup tapes to the off-site storage facility?

- b. By what mechanism will you identify the backup tapes at the off-site storage facility?

- c. Does the rotation schedule listed above include the following?

All backup tapes \_\_\_\_\_  
 Only application backups \_\_\_\_\_  
 Only operating system backups \_\_\_\_\_

- d. How often do the operating system backups occur? (For example, daily, weekly, and so forth)

- e. How are tapes sent to the recovery site identified? (For example, pull list, microfiche, verbal, and so forth)

- f. Please provide the total time to identify, pack, and ship tapes to the recovery site.

- g. Please indicate the number of backup generations sent to the recovery site on the first shipment.

- h. How are tapes shipped to the recovery site?

4. Please identify the backup management system you use. (for example, manual, automated, DFHSM, and so forth.)

- a. Are account data sets under a management system's control?

- b. Which types of files are under this control?

- c. Are **any** files under the control of the management system sent to off-site storage?
  - d. List disk types used:
5. Please indicate the total time required to restore the operating system at the recovery site.
6. Please indicate on the chart below what characteristics make up the restored operating system.

Characteristic	Product Name
User Interface (TSO, Windows, etc.)	
Tape Management System	
Scheduling System	
Promotion to Production System	
Interactive Software	
Data Security System	
Program Products	

- What portion of the catalog will you restore? Who will restore the rest?
- Please indicate the maximum age of the recovered operating system characteristics.

## Output Processing Assessment

1. List below the type of input, the host site, and the method (for example, tape, network, and so forth) by which you receive input (that is, the information from which you produce output).

Input	Host Site	Method

2. Are microfiche/microfilm services processed on-line, off-line, or both?
3. How will delivery services be provided?
4. Identify any special output processing issues.

## Building Assessment

1. Where are the main power switches?
2. Who services the air conditioner?
3. Who services the electrical system?
4. How do you turn off the water main? How would you get a tank truck of water in an emergency?
5. Where is the gas meter turn-off (if any)? Where are the gas lines?
6. Where are the fire extinguishers or other fire suppression systems? Who is trained in how to use them? Who maintains the equipment?
7. Is the building equipped with an automatic sprinkler system? If so, where are the control (cut-off) valves located?
8. What hazardous or flammable materials are stored in the building? Where?
9. Describe building security under normal conditions? What special provisions will be made to protect computer rooms and other sensitive areas if a disaster occurs?
10. Where are the emergency exits? Do the emergency lights work?

<p><i>Note: Attach a building diagram indicating the key systems and areas described above.</i></p>
---

## Bomb Threat Checklist

Use the following checklist if you receive a bomb threat over the phone. Be calm and courteous. Listen carefully to the caller; do not interrupt. Notify your supervisor or a security officer while the caller is still on the line. Get as much information as possible from the caller.

Your name: \_\_\_\_\_

Date of call: \_\_\_\_\_ Time of call: \_\_\_\_\_

### About the Caller

☐ Adult ☐ Juvenile ☐ Male ☐ Female

Caller's Voice: Check all that apply.	Background Noises: Check all that apply.
<input type="checkbox"/> Calm	<input type="checkbox"/> Quiet
<input type="checkbox"/> Rational	<input type="checkbox"/> Voices
<input type="checkbox"/> Slow	<input type="checkbox"/> Radio
<input type="checkbox"/> Soft	<input type="checkbox"/> Street traffic
<input type="checkbox"/> High-pitched	<input type="checkbox"/> Trains
<input type="checkbox"/> Clear	<input type="checkbox"/> Party
<input type="checkbox"/> Well spoken	<input type="checkbox"/> Office
<input type="checkbox"/> Raspy	<input type="checkbox"/> Machines
<input type="checkbox"/> Laughing	<input type="checkbox"/> Other _____
<input type="checkbox"/> Pleasant	<input type="checkbox"/> Other _____
<input type="checkbox"/> Nasal	<input type="checkbox"/> Other _____
<input type="checkbox"/> Angry	
<input type="checkbox"/> Irrational	
<input type="checkbox"/> Fast	
<input type="checkbox"/> Loud	
<input type="checkbox"/> Deep	
<input type="checkbox"/> Disguised	
<input type="checkbox"/> Stuttering	
<input type="checkbox"/> Slurred	
<input type="checkbox"/> Emotional	
<input type="checkbox"/> Foul language	
<input type="checkbox"/> Accent	

### Questions to Ask

When is the bomb going to explode?

Where is the bomb?

What does it look like?

What kind of bomb is it?

What will cause the bomb to explode?

Did you place the bomb? Why?

Where are you calling from?

What is your name? Your address?

Additional information:

## Chemical and Biological Agent Procedures

Whenever a hazardous material is released into the environment, health problems may occur. A chemical or hazardous material contamination may require medical attention immediately. Report to emergency personnel, security, and management as soon as possible and follow their instructions.

### ***Immediate Response***

If you believe that you have been exposed to a biological contaminant:

1. Remain calm. This is very important to your safety and the safety of others.
2. Notify security.
3. Call the local emergency number for your area.
4. Contain the substance if possible. If not contained, evacuate the area of the exposure.

### ***Warning Signs***

- A bag or package left unattended in any building lobby, workspace or loading dock.
- Unusual mail or packages, smudged envelopes, excessive postage, crudely handwritten addresses, no return address, and sloppy wrappings or packaging.

### ***Anthrax - Center of Disease Control (CDC) Guidelines***

The following is a CDC Health Advisory, which was distributed via Health Alert Network on October 12, 2001, 21:00 EDT (9:00 PM EDT):

Many facilities in communities around the country have received anthrax threat letters. Most were empty envelopes; some have contained powdery substances. The purpose of these guidelines is to recommend procedures for handling such incidents.

1. Do not panic.
2. Anthrax organisms can cause infection in the skin, gastrointestinal system, or the lungs. To do so, the organism must be rubbed into abraded skin, swallowed, or inhaled as a fine, aerosolized mist. Disease can be prevented after exposure to the anthrax spores by early treatment with the appropriate antibiotics. Anthrax is not spread from one person to another person.
3. For anthrax to be effective as a covert agent, it must be aerosolized into very small particles. This is difficult to do, and requires a great deal of technical skill and special equipment. If these small particles are inhaled, life-threatening lung infection can occur, but prompt recognition and treatment are effective.

For suspicious unopened letters or packages marked with threatening messages such as 'anthrax', do the following:

1. Do not shake or empty the contents of any suspicious envelope or package.
2. Place the envelope or package in a plastic bag or some other type of container to prevent leakage of contents.
3. If you do not have any container, then cover the envelope or package with anything (for example, clothing, paper, trashcan, and so forth) and do not remove this cover.

4. Then leave the room and close the door, or section off the area to prevent others from entering (i.e., keep others away).
5. Wash hands with soap and water to prevent spreading any powder to your face.
6. What to do next...
  - If you are at home, then report the incident to local police.
  - If you are at work, then report the incident to local police, and notify your building security official or an available supervisor.
7. List all people who were in the room or area when this suspicious letter or package was recognized. Give this list to both the local public health authorities and law enforcement officials for follow-up investigations and advice.

For envelopes with powder and for powder that spills onto a surface:

1. Do not try to clean up the powder. Cover the spilled contents immediately with anything (e.g., clothing, paper, trash can, etc.) and do not remove this cover.
2. Then leave the room and close the door, or section off the area to prevent others from entering (i.e., keep others away).
3. Wash hands with soap and water to prevent spreading any powder to your face.
4. What to do next...
  - If you are at HOME, then report the incident to local police.
  - If you are at WORK, then report the incident to local police, and notify your building security official or an available supervisor.
5. Remove heavily contaminated clothing as soon as possible and place in a plastic bag or some other container that can be sealed. This clothing bag should be given to the emergency responders for proper handling.
6. Shower with soap and water as soon as possible. *Do Not Use Bleach Or Other Disinfectant On Your Skin.*
7. If possible, list all people who were in the room or area, especially those who had actual contact with the powder. Give this list to both the local public health authorities so that proper instructions can be given for medical follow-up, and to law enforcement officials for further investigation.

Room contamination by aerosol (example: small device triggered, warning that air handling system is contaminated, or warning that a biological agent released in a public space):

1. Turn off local fans or ventilation units in the area.
2. Leave area immediately.
3. Close the door, or section off the area to prevent others from entering (i.e., keep others away).
4. What to do next...
  - If you are at HOME, then *dial “911”* to report the incident to local police and the local FBI field office.
  - If you are at WORK, then *dial “911”* to report the incident to local police and the local FBI field office, and notify your building security official or an available supervisor.
5. Shut down air handling system in the building, if possible.
6. If possible, list all people who were in the room or area. Give this list to both the local public health authorities so that proper instructions can be given for medical follow-up, and to law enforcement officials for further investigation.

How to identify suspicious packages and letters:

Some characteristics of suspicious packages and letters include the following...

- Excessive postage
- Handwritten or poorly typed addresses
- Incorrect titles
- Title, but no name
- Misspellings of common words
- Oily stains, discolorations or odor
- No return address
- Excessive weight
- Lopsided or uneven envelope
- Protruding wires or aluminum foil
- Excessive security material such as masking tape, string, etc.
- Visual distractions
- Ticking sound
- Marked with restrictive endorsements, such as “Personal” or “Confidential”
- Shows a city or state in the postmark that does not match the return address

#### Frequently Asked Questions About Anthrax from the CDC

1. What is anthrax?

Anthrax is an acute infectious disease caused by the spore-forming bacterium *Bacillus anthracis*. It most commonly occurs in mammal such as cattle, sheep, goats, camels and antelopes, but can also occur in humans when they are exposed to infected animals or tissue from infected animals.

2. How common is anthrax and who can get it?

Anthrax is most common in agricultural regions where it occurs in animals. Humans infected with anthrax usually have been exposed to infected animals or their products through their occupations. Workers who are exposed to dead animals and animal products from other countries where anthrax is more common may become infected with *Bacillus anthracis*.

3. How is anthrax transmitted?

Anthrax infection can occur in three forms: cutaneous (skin), inhalation, and gastrointestinal. Spores can live in the soil for years, and humans can become infected with anthrax by handling products from infected animals or by inhaling anthrax spores from contaminated animal products. Eating undercooked meat from infected animals also can spread the disease.

4. What are the symptoms of anthrax?

They vary depending on how the disease was contracted, but symptoms usually occur within seven days.

*Cutaneous:* About 95 percent of anthrax infections occur when the bacterium enters a cut or abrasion on the skin, such as when handling contaminated wool, hides, leather or hair products of infected animals. It begins as a raised itchy bump that resembles an insect bite, but soon turns into a painless

ulcer, usually one to three centimeters in diameter, usually with a black center in the middle. Lymph glands in the adjacent area may swell. About 20 percent of untreated cases result in death.

*Inhalation:* Initial symptoms may resemble a common cold, but lead to severe breathing problems and shock after several days. Inhalation anthrax is usually fatal.

*Intestinal:* This form of anthrax may follow the consumption of contaminated meat and is characterized by an acute inflammation of the intestinal tract. Initial signs include nausea, loss of appetite, vomiting and fever, followed by abdominal pain, vomiting blood and severe diarrhea. Between 25 percent and 60 percent of these cases are fatal.

5. Where is anthrax usually found?

Anthrax is global. It is more common in developing countries or countries without veterinary public health programs. Certain regions of the world (South and Central America, Southern and Eastern Europe, Asia, Africa, the Caribbean, and the Middle East) report more anthrax in animals than elsewhere.

6. Can anthrax be spread from person to person?

Direct, person-to-person spread of anthrax is extremely unlikely. It is not contagious.

7. Is there a treatment for anthrax?

Doctors can prescribe effective antibiotics. To be effective, treatment should be initiated early. If left untreated, the disease can be fatal.

8. Is there a way to prevent infection?

In countries where anthrax is common and vaccination levels of animal herds are low, humans should avoid contact with livestock and animal products and not eat meat that has not been properly prepared.

In addition, an anthrax vaccine has been licensed for use in humans. It is reported to be 93 percent effective.

9. What is the anthrax vaccine?

The vaccine is a cell-free filtrate vaccine, which means it contains no dead or live bacteria in the preparation. Anthrax vaccines intended for animals should not be used in humans.

10. Who should get vaccinated against anthrax?

Immunization practices recommend vaccination for the following:

- People who work directly with the organism in the laboratory
- People who work with imported animal hides or furs in areas where standards are insufficient to prevent exposure to anthrax spores
- People who handle potentially infected animal products in high-incidence areas
- Military personnel deployed to areas with high risk for exposure to the organism (as when it is used as a biological warfare weapon)
- Pregnant women should be vaccinated only if absolutely necessary

## Threat and Vulnerability Worksheet

### Part 1—Identify Risks

1. List the possible threats to the site.
2. Examine each threat. Do the threats have a high, medium, or low likelihood of occurrence at your site? Check the appropriate answer in the Likelihood column.
3. What is the vulnerability of your site to this threat? Given all you know about the vulnerability of your site, does the threat present a potential disaster (high) or just a minor incident (low)? Check the appropriate box in the Vulnerability column.
4. Which are the worst threats to your account? The worst threats are those that have a high or medium likelihood of happening and a high or medium vulnerability. These are your risks. Place a check in the Risks column to indicate your worst threats.

### Part 2—Evaluate Risks

1. Indicate which alternatives could be applied to deal with your risks. Check the appropriate box(es): Eliminate (E), Reduce (R), Transfer (T), Accept (A).
2. Evaluate the alternatives based on the evaluation criteria.
3. Prioritize your risks by ranking them in order of importance with one being the risk that would result in the greatest damage or loss.

Possible Threat	Likelihood			Vulnerability			Risks	Alternatives				Rank
	H	M	L	H	M	L		E	R	T	A	

## Community Resources Worksheet

Contact	Phone Number	Secondary Phone Number
Fire Chief		
Police Chief		
Head of Public Works Department		
City Emergency Program Manager		
Local hospital(s)		
Utility Company Representatives: <ul style="list-style-type: none"><li>• Power</li><li>• Water</li><li>• Gas</li><li>• Telephone</li></ul>		
Facilities Manager for your location		

## Customer Meeting Topics

Below are some suggested topics for a meeting, or series of meetings, with the customer. Modify these to fit the needs of the situation. Include other experienced personnel in the meeting who can communicate effectively with both technical and non-technical customers about recovery planning options. Soon after the meeting, document what was discussed and send it to the customer for verification. This is simply a step to ensure accuracy and show the customer that what was discussed is understood.

*Note: Many of these questions could be answered by performing a thorough risk analysis and business impact analysis.*

1. Introduce business continuity planning to the customer.
  - What is it?
  - Why is it important?
2. Discuss customer's role and value to the process.
3. Review customer's business functions and processes.
  - Which processes are critical?
  - For which processes does the customer have an alternate manual process?
  - Would the customer like our assistance in coming up with alternate processes for those areas we currently do not support? (Opportunity to increase business.)
  - Which processes does EDS support?
  - Is there an established maximum downtime for the processes that EDS supports?
  - What is the effect of an interruption to the process?
  - Which processes can be temporarily suspended?
4. Discuss at what point might the customer face governmental, legal, or regulatory fines or sanctions.
5. Discuss what the customer perceives as their biggest risks.
6. Explain EDS' commitment to protecting the customer's business and ask for their participation.
7. Emphasize developing the best strategies to protect the customer's business.
  - Review alternate processing possibilities.
  - Stress importance of customer's security and peace of mind.
8. Explain testing strategies.
  - Explain that test plans will mirror disaster scenarios approved by the customer.
  - Stress importance of customer participation.

## **Crisis Management Plan Outline**

- I. Purpose, Scope, and Objectives
- II. Assessment Checklist
- III. Contact Lists
  - A. Community Resources
  - B. EDS Resources
  - C. Customers
  - D. Vendors
- IV. Communication Procedures
  - A. Account to Customer
  - B. Team to Account
  - C. Account to Team
  - D. Account to Media
  - E. Account to Family
  - F. Account to EDS
- V. Team Safety Plan
  - A. Evacuation Plan
  - B. Preparation and Response Procedures
  - C. Recovery Procedures
- VI. Property Protection Plan
  - A. Emergency Power-Down Procedures
  - B. Emergency Computer and Computer-Room Access Procedures
  - C. Property Recovery Procedures
  - D. Records Management Plan
  - E. Facilities Checklist
- VII. Training Plan
- VIII. Test Plan
- IX. Maintenance Plan

### **Supporting Documentation:**

- Risk Analysis and Business Impact Analysis
- Fixed Assets, PICS, and BIIS reports

## Employee Communication Procedure

Contact **one** of the following (in sequence) until someone has been notified:

<b>Immediate Supervisor or Manager</b>	Office	
	Home	
<b>Account Manager</b>	Office	
	Home	
<b>Other Office Contact (or designated answering machine)</b>		
<b>EDS Physical Security Office</b>		
<b>EDS Disaster Line</b>		
<b>EDS Corporate Switchboard</b>		
<b>Message Drop-off Point</b>		

## Employee Contact Sheet

Name

EDS Phone

Home Address

Home Phone

General Directions From  
(add your work location  
here)

R = Right

L = Left

Cellular Phone

Other Means of Contact

Emergency Out-of-State  
Contact

## Employee Recovery Needs Assessment

**Date:** \_\_\_\_\_ **Time:** \_\_\_\_\_ **Operator:** \_\_\_\_\_

Caller name: \_\_\_\_\_

Phone Number: \_\_\_\_\_

Location: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

How can you be reached? \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

<u>Status</u>	<u>Needs</u>	<u>Needs</u>
_____ Injuries	_____ Medical	_____ Movers
_____ House Uninhabitable	_____ Water	_____ Storage
_____ Severe Damage	_____ Food	_____ Generator
_____ Moderate Damage	_____ Shelter	_____ Chain Saw
_____ House OK	_____ Toiletries	_____ Clean up
_____ Phone Working	_____ Child Care	_____ Roofing Materials
_____ Available to Assist	_____ Transportation	_____ Propane

Specifics: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Do you know the status of others affected by this disaster? \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## Team Safety Assessment

### General Items

Below are some general questions to help assess the emergency resources available in the area.

√	General Threat Questions
	Is there a 911 emergency system in your area?
	Is there reliable, short-distance public transportation, such as buses, trains, taxis, etc.?
	Is there reliable, long-distance public transportation, such as trains, airplanes, etc.?
	How close to your site is police/fire protection located? (Proximity may prevent excessive damage.)
	What is average police/fire/ambulance response time to facilities?
	Is there a local bomb squad?

### Evacuations

Developing and practicing evacuation procedures are an important part of reducing risk. Below are some questions to ask concerning evacuations.

√	Evacuation Questions
	Are there set evacuation procedures?
	Are evacuation procedures posted where all employees can see them?
	Are exit signs properly placed and visible?
	How many occupants and disabled persons are in an assigned area?
	Is there a team established to conduct periodic evacuation drills and equipment tests and to assist in a controlled and safe site evacuation?
	Are evacuations routinely practiced? When was the last time you executed an evacuation drill?
	Are there procedures for a headcount of evacuated personnel?

## Training Topics

Below are some suggested training topics to cover in your response plan training:

Audience	Topic
All Employees	<ul style="list-style-type: none"> <li>• <i>Hazards that may threaten their facility</i></li> <li>• <i>Warning signals and notification procedures</i></li> <li>• <i>Communication throughout the disaster</i></li> <li>• <i>General emergency procedures: fire, medical, etc.</i></li> <li>• <i>Location and use of common emergency equipment</i></li> <li>• <i>Emergency power-down procedures</i></li> <li>• <i>Security procedures for their own work areas</i></li> <li>• <i>Evacuation procedures for their building and site</i></li> </ul>
Special Support Teams	<ul style="list-style-type: none"> <li>• <i>What threats they are and are not to deal with</i></li> <li>• <i>Procedures for handling specific threats: fire, bomb, and medical</i></li> <li>• <i>Whom to contact and how to work with the agency in charge</i></li> <li>• <i>How to lead a building evacuation</i></li> <li>• <i>How to use special emergency equipment</i></li> <li>• <i>How to check for contamination and how to dispose of contaminated clothing</i></li> <li>• <i>Automatic systems to check in an emergency</i></li> <li>• <i>How to activate automatic systems manually and what to do if they can't be activated</i></li> <li>• <i>How to report status</i></li> </ul>

## Problem Log

Date \_\_\_\_\_ Recorded by: \_\_\_\_\_

What time did the problem occur? \_\_\_\_\_

What time was the problem fixed? \_\_\_\_\_

Who fixed the problem? \_\_\_\_\_

Describe the problem:

What was done to fix the problem?

What is the current status?

What is the long-term solution? (Review at the test debriefing.)

## **Public Relations Guidelines**

Public relations considerations should be a part of the business continuity plan. One of the major problems in any emergency, aside from the emergency itself, is the almost immediate attention it will draw from the news media. Reporters will attempt to contact anyone who can give them the information they seek. Below are some guidelines from EDS Public Relations for handling media inquiries:

- All inquiries, whether by phone or in person, should be referred to the EDS Public Relations Office in Plano at (972) 605-6791.
- The attitude toward the news media should always remain professional. Be polite but firm. Say, "All information will be distributed by the EDS Public Relations Office in Plano, Texas. Please call them at (972) 605-6791."
- Do not say, "No comment." It sounds as if something is being hidden.
- Do not provide information "off the record." Anything that is said to reporters at any time may be used in their report.
- Do not rudely hang up on a reporter.

The goal is not to keep information from the media, but to release only high-quality accurate information.

## Recovery Plan Outline

- I. Purpose, Scope, and Objectives
- II. Contact Lists and Procedures
  - A. Customer
  - B. Recovery Team Members
  - C. EDS Resources
  - D. Vendors
  - E. Others
- III. Detailed Recovery Plan (categories and procedures will differ depending on services provided)
  - A. Applications
  - B. Operating Environment
  - C. Telecommunications
  - D. Output Processing
  - E. Manual Processing
  - F. Logistical Support
- IV. Recovery Scenarios
  - A. Disaster Site
  - B. Recovery Site
  - C. Lost Service Provider
  - D. Return to Normal
- V. Test Plan
- VI. Maintenance Plan

### Supporting Documentation:

- Risk Analysis
- Business Impact Analysis

## Recovery Planning Team

Below are guidelines regarding the composition and responsibilities of a recovery planning team. The type of team you set up will vary based on the size and nature of your account.

Table 7.1 – Composition of Team

Role	Responsibilities
Customer	<ul style="list-style-type: none"> <li>Establishes requirements</li> <li>Reviews plans</li> <li>Develops reaction plans for customer staff</li> <li>Participates in testing</li> <li>Designates user representative(s)</li> </ul>
Customer/User Representative(s)	<ul style="list-style-type: none"> <li>Represents customer and users</li> <li>Writes or coordinates recovery plan for customer</li> <li>Participates in testing</li> </ul>
Account Manager	<ul style="list-style-type: none"> <li>Establishes team</li> <li>Gathers requirements from customer</li> <li>Develops recovery strategies</li> <li>Negotiates vendor participation</li> <li>Reviews progress with project leader, manager, and customer</li> <li>Devises testing strategies and participates in testing</li> <li>Ensures that recovery plan is maintained</li> </ul>
Project Leader	<ul style="list-style-type: none"> <li>Develops work plans and schedules based on recovery life cycle</li> <li>Coordinates meetings; reports status</li> <li>Reviews summary questions and recovery time estimates from service providers</li> <li>Coordinates testing</li> <li>Maintains detailed recovery plan</li> <li>Compiles account recovery plan</li> </ul>
Support Staff	<ul style="list-style-type: none"> <li>Supplies administrative support as needed</li> <li>Creates and maintains all contact lists</li> </ul>
EDS Support Group Representatives	<ul style="list-style-type: none"> <li>Represents support organizations that provide key services to the account, for example:               <ul style="list-style-type: none"> <li>Information Processing Centers (IPCs)</li> <li>Data Centers</li> <li>Infrastructure Services</li> <li>Client/Server Group</li> </ul> </li> <li>Devises recovery strategies</li> <li>Writes or coordinates detailed recovery plans for their organization</li> <li>Completes summary questions and recovery time estimates</li> <li>Creates testing strategies</li> <li>Participates in testing</li> <li>Maintains detailed recovery plans</li> </ul>

## Recovery Strategy Meeting Agenda

Below is a suggested agenda for a recovery strategy meeting, or series of meetings, with your EDS internal service providers. Feel free to modify it to fit the needs of your account.

1. Introduction
  - a. Go over the purpose of the meeting.
  - b. Provide an overview of the customer's business and risks.
2. Go over the analysis documentation.
  - a. Review all of the services and products that EDS provides to the customer.
  - b. Review the customer's maximum downtime and other requirements.
  - c. Confirm all service providers.
3. Set strategies.
  - a. Draw a process flow to show how each provider fits into the "big picture."
  - b. Identify dependencies.
  - c. Review various disaster scenarios (including those where the service providers are disabled).
  - d. Discuss possible recovery strategies.
4. Consider mitigation alternatives.
  - a. Discuss coordination points.
  - b. Identify services or systems that are commonly used by several accounts and determine the decision makers and strategies for recovering those services or systems.
  - c. Consider current contracts with disaster recovery vendors, particularly those you have in common.
  - d. Review any procedures that service provider groups have established for dealing with their organizations.
  - e. Share information about internal groups who can assist with the recovery planning effort.
5. Conclusion
  - a. Summarize meeting decisions.
  - b. Explain the ongoing process.
  - c. Review responsibilities.

**Note:** Ask the service providers to hold off implementing any alternate strategies until you get customer approval.

## Recovery Team Responsibilities

In this example, recovery teams are organized around the major service provider functions that support the customer's business. (A Logistical Support Team has been added.) The organization of the teams is less important than making sure all the important responsibilities are covered.

Recovery Team	Recovery Responsibilities
Applications Team	<ul style="list-style-type: none"> <li>Establishes backup procedures</li> <li>Analyzes and determines starting point from which reconstruction and update processing will begin</li> <li>Designs and creates reconstruction and update plan and coordinates all production file update activity</li> <li>Organizes and controls off-site storage facility</li> <li>Maintains inventory of applications</li> <li>Maintains and improves the plan</li> <li>Maintains ongoing support and development</li> </ul>
Operating Environment Team	<ul style="list-style-type: none"> <li>Acquires and installs backup system hardware and software</li> <li>Examines and maintains operating system software, security systems, utility programs, and production files on backup computer system to assist in reconstruction and update process as well as the recovery itself</li> <li>Maintains inventory of system hardware and software</li> <li>Maintains and improves the plan</li> </ul>
Telecommunications Team	<ul style="list-style-type: none"> <li>Reinitializes data and voice communications at original site, or moves them to alternate site</li> <li>Installs communications software modules</li> <li>Assists in examining circuits and devices</li> <li>Maintains telecommunications inventory</li> <li>Maintains and improves the plan</li> </ul>
Output Processing Team	<ul style="list-style-type: none"> <li>Ensures backup printing equipment is working at original or alternate site</li> <li>Acquires necessary forms or other supplies</li> <li>Maintains inventory of output equipment and supplies</li> <li>Maintains and improves the plan</li> </ul>
Manual Processing Team	<ul style="list-style-type: none"> <li>Ensures manual processing continues</li> <li>Responsible for temporary personnel, alternate work site and procedures, equipment, and supplies</li> <li>Maintains inventory of equipment and supplies</li> <li>Maintains and improves the plan</li> </ul>
Logistical Support Team	<ul style="list-style-type: none"> <li>Coordinates alternate processing site including physical security</li> <li>Creates and maintains contact lists and inventory of supplies</li> <li>Secures office space (and possibly housing) for personnel</li> <li>Provides logistical support, including transportation of material, supplies, equipment, and personnel</li> <li>Provides administrative support</li> <li>Maintains and improves the plan</li> </ul>

## Service Provider Questions

Name of Service Provider \_\_\_\_\_

Address \_\_\_\_\_

Contact Name \_\_\_\_\_ Phone \_\_\_\_\_

Prepared By \_\_\_\_\_ Date \_\_\_\_\_

1. Is each service you are responsible for covered by a detailed recovery plan?  
If no, explain why not and indicate when a plan will be available.

2. Please provide the location of the recovery (alternate processing) site below.

Name of Facility \_\_\_\_\_

Address \_\_\_\_\_

City/State \_\_\_\_\_

Contact Name \_\_\_\_\_ Phone \_\_\_\_\_

Duration of Agreement/Contract \_\_\_\_\_ Renewal Date \_\_\_\_\_

3. If off-site storage exists, please provide the location of the facility below.

Name of Facility \_\_\_\_\_

Address \_\_\_\_\_

City/State \_\_\_\_\_

Phone \_\_\_\_\_

Contact \_\_\_\_\_

## Telecommunications Services

1. If your network system supports any channel-extended attached sites, please identify those locations and providers below.

Location	Network Provider

2. If it is necessary to recover in multiple locations, please list those account names, locations, and contact information below.

Account Name	Location	Contact Name & Phone

- a. Describe the situations that cause multiple-site recovery.

3. If the primary processing site fails, how will you support the following:
  - a. Applications running at an alternate recovery site?
  - b. Alternate connectivity to the recovered applications?
  - c. Routing of output from the recovered applications to the output centers?
  - d. Connectivity of applications to various remote processing sites?
  - e. The account support groups?
  - f. The application system groups?
4. How will the end-user be recovered if the dedicated link fails?
5. How will the output requirements be supported if the links to the output processing center fail?
6. How will the remote processing center's requirements be supported if links to them fail?
7. How will access to applications running at other EDS IPCs be supported if the links fail?

## **Test Plan – Executive Summary**

- I. Account Information
  - A. Account Name
  - B. Location
  - C. Manager
  - D. SBU
  - E. Test Coordinator
- II. Test Scope
  - A. Test Dates
  - B. Location
  - C. Scenario
  - D. Participants
  - E. Objectives
- III. Test Results Summary
  - A. Objectives Met
  - B. Significant Events/Accomplishments/Problems
  - C. Time Spent
  - D. Lessons Learned

## Test Results Report

- I. Account Information
  - A. Account Name
  - B. Location
  - C. Manager
  - D. SBU
  - E. Test Coordinator
- II. Test Scope
  - A. Test Dates
  - B. Location
  - C. Scenario
  - D. Participants
  - E. Objectives
- III. Test Results Summary
  - A. Objectives Met
  - B. Significant Events/Accomplishments/Problems
  - C. Time Spent
  - D. Lessons Learned
- IV. Test Logs
  - A. Event Logs
  - B. Problem Logs
  - C. Test Notes
- V. Corrective Action Plan
  - A. Recommendations
  - B. Implementation

## Appendix A: Memo of Understanding

---

The following memo documents an agreement between the Indiana Solution Centre and the Indiana Title XIX account. In the event of a disaster, the Indiana Title XIX account may utilize Indiana Solution Centre facilities as a temporary work location.


	<h1>Memorandum</h1>
To:	Rick Shaffer EDS Indiana Title XIX 950 N Meridian, Suite 1150 Indianapolis, IN 46204
From:	Nelson Martin EDS Indiana Solution Centre 2601 Fortune Circle East, Suite 100C Indianapolis, IN 46241
CC:	Ronald Koger Business Continuity Plan Project Leader 950 N Meridian, Suite 1150 Indianapolis, IN 46204
Date:	January 28, 2003
Subject:	Business Continuity Planning
<hr/>	
<p>The purpose of this memorandum is to document an agreement for the Indiana Solution Centre to provide aid to the EDS account at Indiana Title XIX in the event of a disaster.</p> <p>If a disaster occurs at the Indiana Title XIX facility, account personnel may use available space at Indiana Solution Centre facilities in Indianapolis as a temporary worksite while disaster recovery operations are in progress. The Indiana Title XIX account may list Indiana Solution Centre facilities as alternate worksites in their Business Continuity Plan.</p> <p>If you have any questions, please contact Nelson Martin at 317-240-5565.</p>	

Figure A.1 – Memo of Understanding



## ***Appendix B: Back-ups and Offsite Storage***

---

The EDS obligation to back up the Indiana interChange System and all its data can be found in sections 4.5.5 and 5.4.14 of the EDS contract. These sections read as follows:

### **Excerpted from section 4.5.5 of EDS contract**

EDS performs incremental backups each evening and full backups every Sunday. Copies are retained on-site and are also sent to the Iron Mountain off-site storage facility. Recoveries are performed by using the backup tapes from Iron Mountain, if unavailable on-site. In a recovery, the appropriate files are reloaded from the weekly full backup, and then the appropriate daily incremental backups are used to restore the system to current processing status.

### **Excerpted from section 5.4.14 of EDS contract**

EDS supports routine system and database backups. We have established procedures for the process of performing backups. On a weekly basis, we do full backups of all software and operating programs, databases, and system files. To supplement the full backup and protect against any loss of data, incremental system backups are performed on a daily basis. Additionally, we perform a full backup of the file server on a daily basis. All backups are stored at an off-site facility to protect against loss in the event of a disaster.

In addition to routine operating system and database backups, we archive databases transaction logs. Archiving transaction log information is of the utmost importance in the event that a database must be restored. In the event of a failure, a database can not be restored without the database transaction history. As such, EDS archives these transaction logs twice a day to ensure that we have the most current data should restoration become necessary.

Through the process of performing routine back-ups, we have the ability to restore any data that has been backed-up. Although tapes are stored at an off-site facility, EDS can recall tapes at anytime. In situations where data has been lost or corrupted, data can be restored. This process begins by recalling the tape from the off-site facility. Once the tape is returned to EDS, the restoration is performed.

EDS Indiana Title XIX has a written Purchase/Lease Order with Iron Mountain. Iron Mountain maintains secure offsite storage of computer backups and EDS documents. A copy of the Purchase/Lease Order can be found at Iron Mountain or EDS Indiana Title XIX.



## Appendix C: Site Risk Analysis

### Overview

The first step to prepare for disasters at the EDS Indiana Title XIX facility is to identify hazards and potential threats. Identifying risks that might affect the account allows identification of the way people, business, assets, and structures may be damaged by a disastrous event. This identification shows the account's areas of vulnerability.

Only the hazards considered threats to this site are addressed in the risk analysis provided in this section.

### Threat/Vulnerability Worksheet

Table C.1 – Threat/Vulnerability Worksheet

Possible Threat	Likelihood				Vulnerability				Priority Risks
	H	M	L	NA	H	M	L	NA	Worst Threats
Earthquake			X		X				
Hurricane				X				X	
Tornado/Wind Storm	X				X				4
Flood			X		X				
Winter Storm		X					X		
Landslide				X				X	
Severe Thunderstorm			X				X		
Epidemic			X				X		
Telecommunications	X				X				2
Explosion			X				X		
Gas Leak		X					X		
Water Pipe Break		X			X				
Structural Fire		X			X				5
Power Failure	X				X				1
Climate Control Failure (heat, air, and so forth)	X					X			
Hardware Failure	X					X			
Software Failure		X				X			
Media Failure (tape, DASD, and so forth)		X				X			
Inadequate Facility Wiring			X				X		
Bomb Threat		X			X				
Civil Disturbance		X					X		

(Continued)

Table C.1 – Threat/Vulnerability Worksheet

Possible Threat	Likelihood				Vulnerability				Priority Risks
Sabotage/Virus	X				X				3
Theft			X				X		
Organized Labor Dispute			X				X		
Computer Crime			X				X		
Data Entry Error			X				X		
Improper Handling of Sensitive Data	X					X			
Unauthorized Access or Theft of Data			X				X		
Malicious Damage of Property			X			X			
Loss of key Personnel		X					X		
Volcanic Hazards				X				X	
Hazardous Materials Release	X					X			
Transportation Accident		X				X			
Electromagnetic Interference	X					X			
Nuclear Attack		X			X				

Table C. 2 – Risk Priorities

Risk Priority	Reason	Possible Alternatives
1. Power Failure	Utility company cut power or ice storm	<ul style="list-style-type: none"> <li>• Process manually</li> <li>• Operate at alternate site</li> <li>• Use power supply backup</li> <li>• Follow posted power-up or down procedures by equipment</li> <li>• Use surge protectors or power conditioners</li> </ul>
2. Telecommunications	Insufficient backup procedures or outage	<ul style="list-style-type: none"> <li>• Use power failure phones</li> <li>• Switch recovery for SFD</li> <li>• Use battery backup</li> <li>• Use radio</li> <li>• Use alternate routings</li> </ul>

(Continued)

Table C. 2 – Risk Priorities

<b>Risk Priority</b>	<b>Reason</b>	<b>Possible Alternatives</b>
3. Sabotage or Virus	Disgruntled employee or virus	<ul style="list-style-type: none"> <li>• <i>Install software virus check</i></li> <li>• <i>Remove and lockup keyboards</i></li> <li>• <i>Use fiber optics to reduce exposure points</i></li> <li>• <i>Ensure terminals are not left unattended</i></li> <li>• <i>Deactivate LAN servers by removing keyboards and A:\ drives</i></li> <li>• <i>Use call-back modems</i></li> </ul>
4. Tornado or Wind Storm	Site located in tornado or windstorm belt	<ul style="list-style-type: none"> <li>• <i>Limit level of service</i></li> <li>• <i>Use alternate site</i></li> </ul>
5. Fire	Fire at the EDS site or elsewhere in building	<ul style="list-style-type: none"> <li>• <i>Ensure fire protection equipment is adequate and properly maintained.</i></li> <li>• <i>Ensure fire department frequently inspects your site.</i></li> <li>• <i>Use alternate site</i></li> </ul>

## Facility Location

The EDS Indiana Title XIX site consists of four office suite areas on the second, ninth, tenth, and eleven floors in a single twelve-story administrative office building. The Gateway Plaza building, constructed in 1988, is shared with several other businesses. The building is located at 950 N. Meridian St in Indianapolis. A site risk analysis encompasses the portion of the actual office building site and the impact of any activities in the local geographic area. The building areas evaluated by this analysis are contained in a building area that covers approximately 20 percent of the building address. The building address is shared with other tenants in the building.

The EDS Indiana Title XIX site is located just north of the center of Indianapolis in an area populated by recently constructed office buildings, hotels, and restaurants. The nearby residential neighborhood consists of lower to medium scale single and multiple family dwellings. Industrial enterprises in the immediate area consist primarily of small and medium sized office structures, small shopping malls, and medium sized hotel facilities. The nearest local manufacturing is based approximately two miles southeast of the site.

The residential neighborhoods to the north, west, and south of the EDS facility, are considered lower to middle-class areas. Many of the homes to the north are multifamily and single-family homes that have been renovated by the rules of the historical society.

The door to the data center area has an electronic locking system. Fire extinguishers are installed within the computer operations room.

The building is made of noncombustible materials; brick, concrete, and steel and the building is in good condition. Foundations are reinforced concrete. Internal frames are made of steel beams, concrete columns, and trusses. The flooring is poured concrete, engineered for normal office usage.

To reduce problems caused by electrical power failures that affect data entry and personal computer equipment, surge suppressors are installed to protect equipment. Special circuits are reconfigured in the EDS area to assure consistent power to the computer room area. Uninterruptible power supplies (UPSs) are installed to protect critical computer room equipment.

There are several fire stations within 1.5 miles of the building which is located at 950 N. Meridian St. The nearest fire station is located approximately .7 miles away at 155 W. 16<sup>th</sup> Street. There is another fire station located approximately .8 miles away at 555 N. New Jersey Street. The third fire station is located approximately 1.5 miles away at 439 W. Ohio Street. All three fire stations are staffed full-time, 24 hours a day.

The Indianapolis Police Department is divided into five districts. The building at 950 N. Meridian St. is located in the Downtown district that is subdivided into seven beats. The headquarters building for the Downtown district is located at 209 E. St. Joseph Street. Patrol cars are directed by radio dispatch to address emergency situations. The EDS site is located in a medium crime-area.

EDS account efforts are focused on the prevention of theft, violence, and breaking and entering. EDS has taken several precautionary measures to address security issues at the site. Electronic access locks are installed on major entrances and a procedure has been developed regarding code changes. The building entrance is restricted to key holders during non-business hours. The building entrance doors are protected by an audible alarm system. The parking lots have pole-mounted lights and building entrances are lighted at night.

## Building Construction

The EDS Indiana Title XIX campus is located on a slight grade, above adjacent parking areas. The parking areas and the building are well drained, using municipal storm sewers. The disaster preparedness team's investigation shows the site's geographic location is exposed to some natural hazards.

## Communication Service Lines

Public dedicated phone lines provide communication service lines interfacing with the EDS Indiana XIX building. With controlled circumstances, the account has participated in testing alternative phone lines.

In the event of a communications disaster that affects lines in the building, EDS Field Services resources, comprised of available technicians, would be used to route, test, and connect communication lines.

## Natural Hazards

Natural hazards are caused by events related to weather extremes and geographic-based risks. At this site, natural hazards include thunderstorms, windstorms, winter storms, earthquakes, extreme heat or cold, floods, tornadoes, and fires.

Weather extremes such as tornadoes, thunderstorms, and winter storms pose the greatest weather threat to this area.

This section provides procedures to follow during various types of natural hazards.

## **Earthquakes**

Seismic maps depict inactive fault evidence in southwestern Indiana. The New Madrid and Wabash Valley fault zones could result in shock waves that would cause extensive damage in Indiana. Because of the history of strong earthquakes with epicenters in Indiana, and because of the presence of compression forces acting on deeply buried faults under the state, it is reasonable to conclude that in addition to threat from the New Madrid zone, Indiana also faces the possibility of the occurrence of a strong quake with an epicenter within its borders. Physical damages have been minimal in the past when earthquakes have occurred. As development accelerates, future damage estimates may rise accordingly.

### **Prevention**

Nothing can be done to prevent this type of natural hazard from occurring. The potential for damage caused by an earthquake can be reduced in the following ways:

- Affix tabletop equipment (such as computers or printers) with industrial strength Velcro or lock downs.
- Identify all utility lines (gas, water, and electric) and appropriate shutoff valves or switches and ensure that appropriate instructions are posted nearby explaining how to shut off these utilities.
- Educate employees on where and how to shutoff utility lines.
- Conduct safety drills.
- Ensure that flashlights, radios, and batteries are on hand.

### **Response**

- Remain calm.
- If indoor, take cover under a sturdy piece of furniture to protect from falling objects. Stay away from objects that can shatter, such as windows, mirrors, or skylights.
- Do not use elevators.
- Check for injuries and attend to them; seek medical help if necessary.
- Check for fires or fire hazards.

### **Recovery**

- Earthquakes range from small to catastrophic. Actions will vary depending upon damage conditions. After shocks can also occur after a quake.
- If problems are related to loss of power, use the procedures outlined later in this section.
- If problems are related to fires and explosions, use the procedures outlined later in this section.
- If conditions arise from flooding or water damage, use procedures outlined later in this section.

In addition, be aware of the following:

- Check gas, water, electric, and water lines.
- If there is a gas smell, open windows or doors and shut off the main gas valve.
- Do not use matches, lighters, or open flame appliances until it is certain there are no gas leaks.
- Do not operate electrical switches or phones, if gas leaks are suspected.
- If electrical hazards are identified, shut off the power source, if possible.

- Do not eat or drink from open containers near shattered glass.
- Check to be sure that sewage lines are intact before permitting toilets to be flushed.
- Avoid using the telephone except for emergency calls.
- Use battery operated radios for damage reports and information.
- Be prepared for aftershocks.

## Volcanoes

Volcanoes do not occur in Indiana.

## Floods

The likelihood of a flood affecting the EDS site is a low probability. The White River is located near the EDS Title XIX building. The main flood season on the White River is normally during April, May, and June. Flooding is caused primarily by rain and snow melt.

### Prevention

- Regular facility inspections are the best prevention from water damage.
- The disaster response facility coordinator performs a quarterly facilities inspection of the areas where account computer resources are located for threats from water damage hazards.

### Response

If flooding is detected, account support personnel should follow these procedures:

- Account processing operation users should contact the landlord in the event of a water line rupture or leak. If possible, turn off the power to all affected systems.

*Note: If electrical power can be shut off without standing in water on the floor, do so. Water on the floor may be energized.*

- If water drips into electrical equipment, have the landlord turn off electrical power immediately at the circuit breaker for that equipment. If the landlord is not available, have the facility coordinator attempt to shut the power off from the electrical room in the main hallway. Cover equipment with plastic, if available.
- In case of a small leak, contain it with a wastebasket or comparable receptacle.
- If flooding endangers the computer room or processing in any way, notify EDS management and facilities personnel immediately.
- If appropriate, ask the building owner to turn off the water supply to the affected area or the city water supply to the building.
- In the event of catastrophic damage to the facility, it may not be possible to occupy the area of the facility for several days.
- The communication coordinator, at the direction of the disaster response manager or account manager, should deploy the disaster response computer support, facility, and assessment coordinators to assess the impact of the situation.
- The computer support, facility, and assessment coordinators should make an initial determination of the extent of the damage. Be alert to the electrocution hazards of standing water. Also, be alert to the potential failure of ceiling tiles weighted down from water saturation. The assessment coordinator makes photographic evidence of damage.

- The computer coordinator should evaluate any hardware affected, estimate downtime, and give this information to the assessment coordinator.
- The facility coordinator should estimate the time for repair and clean up.
- The facility and computer support coordinators attempt to protect hardware from additional water damage by removing equipment or blocking further water damage using plastic sheeting or anything else at hand. Immediately remove damp or wet equipment, media, and documents from the hazard site. If diskettes, tapes, or other media are immersed in water when they are found, store them immersed in water. This will allow them to be separated for cleaning and drying, and probable retention of the data contained on them.
- Place items in an air-conditioned area or use blowers or dryers to remove the humidity from the area. Open all covers to allow water to run out of equipment. Fans can also be used to dry equipment. Have a qualified technician remove all cords, and deionize them. Check all circuitry with the appropriate test equipment. Redip or relacquer cards as necessary. Reassemble the unit and power it up. Boot the unit from a floppy disc to test its components. Run diagnostics on the system and replace any failed cards.
- If needed, Blackmon-Mooring-Steamatic Catastrophe Inc., is equipped to handle damage restoration. EDS has a master agreement in place with this company. See *Section 6* for vendor contacts.
- The facility coordinator should use the EDS Business Continuity Planning Guide that clearly defines actions that should be taken to facilitate recovery.
- The assessment coordinator reports to the account or disaster response manager and gives a status report of current conditions and expected duration of the problem.
- The account manager determines if the conditions require a declaration of a disaster after conferring with other senior EDS leaders. The intent of the account support staff in reacting to the situation, such as relocating part or all electronic processing functions during the repair are clarified. The account manager notifies the Office of Medicaid Policy and Planning (OMPP) within 24 hours of the event.
- The disaster response manager determines if the damage to hardware and applications is catastrophic enough to warrant contacting EDS Risk Management.
- If a disaster is declared, the communication coordinator assembles the disaster response team in the safest area away from the danger and develops actions to be taken. If a conference room is not habitable, the team forms in another room onsite. If the site is deemed uninhabitable then the team shall meet at the Holiday Inn – North or Hyatt Regency – Downtown. An action plan is identified based on the account support staff's intent, and reviewed by the EDS leadership team.
- The facility coordinator facilitates the necessary repairs and cleans up to ensure the integrity of the computer hardware after an action plan is identified.
- If a long-term structural repair is likely, move the critical business functions to the alternate processing sites.
- The computer support coordinator with the expertise of Sun or other third party service personnel establishes the integrity of affected hardware. If equipment replacement is required, it is requisitioned through normal EDS channels. If the equipment is critical, an emergency requisition may be necessary through the account manager. Segregate, but do not dispose of, irreparable hardware, it may have to be examined by EDS Risk Management adjusters.
- The computer support coordinator ensures that all electrical contacts are cleaned with a wire brush and that contaminants are removed from connectors. Reseat all connections, and test equipment after powering up. Test all cables with a sniffer or Time Domain Reflectometer (TDR) for opens, shorts, and so forth. As units are added to the LAN, check the system thoroughly. Check everything for intermittent failures or glitches.

- If the movement of some or all of the processing capability is deemed necessary, the disaster response team leader notifies the affected EDS area supervisors.
- Because of the threat of mold attacking the paper on wet documentation, photocopy or scan all damaged documents. Place priority on critical items that cannot be easily acquired elsewhere. This should be done while the documents are within an air-conditioned environment.

*Note: Mold makes documentation unusable within 48 hours, depending on temperature, if not refrigerated. Careful clerical employees should photocopy these documents as assigned by the disaster response team leader.*

- Contact EDS Real Estate to use its services to facilitate an alternate processing and business site.
- Assure the primary or alternate site has the necessary environmental controls (HVAC, fire protection, and electrical power) and voice and data communication.
- Identify the hardware necessary to meet the minimum information processing requirements for critical operations.
- If the hardware within the site is deemed unusable or irreparable, acquire the necessary hardware through EDS-Technical Resource Acquisition's excess equipment listing or through normal purchasing procedures.
- The disaster response team leader and computer support coordinator develop an installation schedule for the facility or at the alternate processing site for the new and relocated hardware.
- The computer support coordinator installs the hardware according to the schedule.
- Obtain any necessary operating supplies.
- The communication coordinator and computer support coordinator coordinate restoration and verification of data communication for the minimum network configuration to support the critical operations. This includes LANs, state networks, and connectivity to any EDS SMCs.
- The communication coordinator requests local telecommunication vendors check the integrity of the communication lines for critical hardware and functionality.
- The disaster response manager directs requests from the account support staff for variations to the critical applications and hardware.
- The disaster response team leader makes arrangements for transportation to and lodging at customer sites (if deemed necessary) for critical personnel if an alternate site is used.
- The disaster response team leader and computer support coordinator develop security procedures for the new site or alternate processing site. EDS Information and Physical Security Departments may assist.
- The disaster response team leader, computer support coordinator, and account support staff determine the synchronization point, most likely the last backup before the water damage.
- The computer support coordinator identifies the backup media required for recovering the operating environments.
- The computer support coordinator identifies the backup media required for recovering the account-owned applications and data in priority sequence.
- Recover the operating system, account-owned applications, and data in priority sequence at the new installation or alternate processing site.
- Verify the operability of the recovered operations.
- Return backup media to storage.

## Recovery

- Obtain account support staff verification of data recovery to the synchronization point after reprocessing lost data.
- The disaster response team leader instructs the affected EDS area supervisors on the need to process data that was created, modified, or deleted while information processing services were not available.
- Perform insurance and salvage activities in the area affected by the damage. EDS Risk Management has the information on the specifics of this function.
- Segregate damaged hardware, office equipment, and so forth.
- Contact Sun maintenance to recertify and determine the reparability of affected hardware. Segregate unsalvageable hardware. Do not dispose of any hardware until EDS Purchasing USA issues EDS scrap forms.
- The computer support coordinator and assessment coordinator quantify the estimated dollar loss associated to the equipment.
- Obtain insurance adjusters authorization to replace or repair equipment.
- The assessment coordinator works with the disaster response team leader to document any losses incurred including all loss-related expenses such as internal labor costs plus burdens, segregating premium from straight time.
- The facility coordinator salvages all usable office equipment, files, and supplies.
- The facility coordinator should use the EDS Business Continuity Planning Guide that clearly defines actions that should be taken to facilitate recovery.
- The facility coordinator obtains a schedule and work plan for rebuilding the primary work area. An occupancy date should also be determined.
- The EDS account manager confers with the OMPP about forthcoming plans to recover the site. During this discussion, all aspects of the contract are reviewed to ensure full compliance and that any needed authorizations from the OMPP are in place.
- The disaster response manager and account manager communicate schedules for recovering suspended and alternate process functions with the account support staff.
- Complete the planning, scheduling, installation, and checking for alternate process as well as suspended activities.
- The disaster response manager schedules the migration from any alternate processing sites to the primary facility.
- Establish a move date in conjunction with the State.
- OMPP representatives actively participate in all meetings held to plan for the recovery of the home site. This ensures effective communication between the two parties and guarantees all contractual obligations are met and approved.
- Establish a curfew period for changes to the operating system, data communication, support programs, production jobs, and data, so they may be backed up for migration back to the primary facility. The disaster response team leader notifies the appropriate EDS supervisors of the scheduled migration.
- Create the necessary backup media for migration from the systems at the alternate processing sites. Necessary application and backup media for restoration is acquired from the vaults and offsite storage.
- Verify the operability of the recovered site by testing equipment functions, software, operating system, telecommunication, and all local terminals.

- Migrate operations in critical-alternate process-suspend order.
- Obtain account support staff verification of data migration.
- Return backup media to storage.
- Coordinate the relocation of offsite personnel.
- Reprocess any data processed manually by the account support staff during the period of time that the electronic data processing functions were affected in the restored system.
- When systems are restored, back them up and immediately store the media offsite.
- The disaster response team leader collects the activity logs from the communication coordinator and the reports from the assessment coordinator.
- The disaster response manager and disaster response team leader critique the team's efforts to find ways to improve future recovery efforts.
- Upon the instruction of the disaster response team leader, based on approval of EDS Risk Management and EDS-TRA Disposition, the facility coordinator disposes of unrepairable hardware.

## **Thunderstorms**

This site is in a low-risk area, with five to 10 storms each year. The months of greatest concern for the EDS Indiana Title XIX site are May, June, and August.

Severe thunderstorms vary in magnitude and strength. They may affect several states or a portion of one state. Thunderstorms create an emergency by impeding the use of resources. Frequently, surface traffic is also impacted and can be halted or routed along less efficient routes. There may be electrical power outages, or damage to communications equipment and processors because of the electromagnetic discharges associated with lightning strikes. Electrical power may be affected by voltage fluctuations and outages, due to damaged power and telephone lines caused by high winds and hail.

The EDS Indiana Title XIX hardware is located throughout the building. Some hardware, software, and other susceptible material is located near exterior walls where the effects of positive ionization from nearby lightning strikes could cause magnetic interference on data storage devices.

### **Prevention**

Nothing can prevent a thunderstorm; however, precautions can be taken to minimize potential damage.

Knowing when a thunderstorm is approaching is one of the best ways to prepare. When a severe thunderstorm warning is issued by the National Weather Service, storms are in the area with lightning or damaging winds greater than 58 miles per hour, hail that could reach a diameter of 3/4 of an inch, and heavy rain.

High-quality power conditioning equipment, such as surge suppressors and UPSs, are used on all LAN and Unix hardware and its peripherals. High-quality power conditioning equipment, such as surge suppressors is used on all workstations and personal computers. Inexpensive power strips do not shunt surges, or interrupt the flow of power that can allow destructive electrical surges and spikes. Nor do they prevent the introduction of noise from fans and other appliances accidentally plugged into the wrong outlet. As a result, internal components of the hardware fatigue, and equipment can be destroyed. This aspect of prevention applies to all natural hazards.

There is an UPS power distribution unit on the computer room floor. It protects against sags and surges and provides a conditioned source of uninterruptible power.

Protective Measure	<p>Protective measures to safeguard personnel and equipment should be taken during lightning activity.</p> <ul style="list-style-type: none"> <li>• If local lightning strikes are imminent, at the instruction of the group supervisor, workstations and PCs should be shutdown, power strips turned off, and the power strip plug pulled from the receptacle (breaking the tie to the building ground).</li> <li>• Individuals should avoid situations that would increase their chances of being struck by lightning. Such situations include, but are not limited to, remaining outdoors in an open area during a storm; remaining under, or close, to tall structures, either natural or man-made, such as water towers or trees.</li> <li>• Hardware, software, and other susceptible materials should not be located against exterior walls where the effects of positive ionization from nearby lightning strikes may cause electromagnetic interference on data-storage devices. Minimum standards for storing these items against an exterior wall are to allow 18 inches between the wall and the stored items.</li> <li>• If local lightning strikes are imminent, the system administrator should advise the system users to frequently save their data.</li> <li>• If local lightning strikes are imminent, the system administrator should perform or wakeup the incremental backup process to perform a data saving pass over the system hierarchy.</li> </ul>
Response	<p>When a thunderstorm disrupts the quality of electrical power or damage from a lightning strike is suspected, notify the EDS operations support personnel disaster response manager immediately.</p> <p>If a significant service interruption is suspected, (one that cannot be resolved by rebooting the system) the following actions should be taken:</p> <ul style="list-style-type: none"> <li>• The communication coordinator, at the direction of the disaster response manager or account manager, contacts the facility, computer hardware, computer application, and assessment coordinators.</li> <li>• The facility coordinator determines the extent of the power outage and feed this information to the disaster response manager.</li> <li>• The computer coordinator and assessment coordinators evaluate affected information processing services and estimate downtime.</li> <li>• The assessment coordinator reports to the account or disaster response manager and give a status report of current conditions and expected duration of the problem.</li> <li>• After conferring with the disaster response team, the account manager determines if conditions require a declaration of a disaster.</li> <li>• In the event of a catastrophic power failure or declared disaster, the disaster response manager will advise the customer accounts. The EDS account and disaster response managers should be fully aware of all contractually obligated time frames for notification to their respective state counterparts.</li> <li>• If a disaster is declared, the communication coordinator assembles the disaster response team in the most secure room or location available to develop actions.</li> <li>• After an action plan is identified, the facility coordinator facilitates the necessary repairs to ensure clean power to the critical hardware. If a long-term power outage is likely, a rental generator should be considered.</li> <li>• The computer coordinator with the expertise of vendor service personnel establishes the integrity of affected hardware.</li> <li>• Lightning strikes, power surges, and electric pulse fluctuations can effect computers in unusual ways. Do not immediately believe that a puzzling hardware problem means replacement is necessary. Attempt to restore what might ordinarily not be necessary. For example; the user</li> </ul>

interface might indicate that a device's baud rate is set for a normal position of 9600. Symptoms of the problem lead you to believe the baud rate is wrong. Reset the baud rate to 2400 or another setting then switch it back.

- If equipment replacement is required, it will be requisitioned through normal EDS channels. If the equipment is critical, an emergency requisition may be necessary through the account manager. Segregate, but do not dispose of, irreparable hardware, as it may have to be examined by EDS Risk Management adjusters.
- The computer support coordinator ensures that users investigate the integrity of the data they were working on at the time of the lightning strike or power fluctuation. They should also be instructed to try several resident applications. Reloading of applications or data is prioritized based on the critical applications listed in this manual.
- The communication coordinator requests local telecommunication vendors check the integrity of the communication lines for critical hardware and functionality.
- Requests from the account support staff for variations to the critical applications and hardware are directed to the disaster response manager.
- In the event of catastrophic power failure it may be necessary for the communication coordinator, at the direction of the disaster response manager, to advise the OMPP and SHC account office in Plano, Texas, on a need to know basis.
- If the lightning strike caused catastrophic hardware damage, the assessment coordinator should take a photographic record of any visible damage such as burned power strips, exploded component on system boards, and so forth.
- The disaster response team leader reports all status information to the disaster response manager.
- The disaster response manager determines if the damage to hardware and applications is catastrophic enough to warrant contacting EDS Risk Management.
- The computer support coordinator should oversee repair work by vendors involving replacement of system boards. Often, when a component on a system board explodes, it can effect the boards adjacent to it. Ensure that vendor technicians check this possibility.
- The effected hardware, software, data, and communication are restored based on the identified prioritization. The disaster response manager and account manager should communicate schedules for recovering suspended and alternate process functions with the account support staff.
- The EDS account and disaster recovery managers coordinate activities with the OMPP to ensure that all contractual obligations are met and approved before bringing the system up for production.
- The disaster response team leader verifies recovery of all processes with the account support staff area managers.
- Any data processed manually by the account support staff during the period of time that the electronic data processing functions were affected will be reprocessed in the restored system.
- When systems are restored they are backed up and the backup media is immediately stored offsite.
- The communication coordinator contacts the SHC account office and customer account personnel and advise them of the completed repair activities.
- The disaster response team leader collects activity logs from the communication coordinator and the reports from the assessment coordinator.
- The disaster response manager and disaster response team leader critique the team's efforts to find ways to improve future recovery efforts.

## Recovery

- Upon the instruction of the disaster response team leader and based on approval of EDS Risk Management and EDS-TRA Disposition, the facility coordinator should dispose of irreparable hardware.
- Return any borrowed or rented equipment.

## Winter Storms

EDS Indiana Title XIX is in a moderate risk area for winter storms. Risks include the effects of heavy ice and snowstorms. Specific hazards are damage to power and telephone lines outside of the building, shutdown of roadways, voltage fluctuations, and secondary damage to power and telephone lines caused by vehicles.

The Indianapolis area is especially prone to ice storms when other areas of the state receive heavy snow because of the thermal mass of the metropolitan area.

Employee absenteeism, injury, and possible loss of life may result from travel hazards. Often major roadways may be impassable for hours, and passage can be restricted for days.

### Prevention

Nothing can be done to prevent a winter storm from occurring; however, prevention can help reduce associated problems.

High-quality power conditioning equipment, such as surge suppressors and uninterruptible power supplies, are used on all LAN and Unix hardware and its peripherals. High-quality power conditioning equipment, such as surge suppressors are used on all workstations and personal computers. Inexpensive power strips do not shunt surges, or interrupt the flow of power that can allow these destructive electrical surges, as well as spikes. Nor do they prevent the introduction of noise from fans and other appliances accidentally plugged into the wrong outlet. As a result, internal components of the hardware fatigue, and equipment can be destroyed. This aspect of prevention applies to all natural hazards.

The EDS Title XIX account should have a snow emergency plan that addresses the general winter weather conditions that follow. Managerial decisions should include consideration of mission critical people and processes. Choose who these people are and what the processes are and arrange for nearby lodging of these people in the event of severe weather conditions.

- If the forecast (usually a National Weather Service advisory about the severity of the coming storm) precedes normal work hours, management may decide to put into effect a stay-at-home policy for those employees who would experience dangerous conditions to arrive at the workplace. As a matter of courtesy, these employees should contact their managers by telephone to inform management of their decision. This situation applies if the National Weather Service declares a snow emergency for the area. Alternatively, those employees who feel they can safely drive through the storm may do so.
- If the forecast coincides with business hours, management monitors weather conditions and decide whether or not to call early hours for non-mission critical employees.
- Ensure that flashlights and radios are on hand with a supply of batteries.
- Ensure that the medical first-aid kit is fully equipped by periodic checks and refurbishing as needed.
- Have a supply of matches, candles, and lanterns available.
- Perform a full file back-up of the Sun system.
- Back-up individual PC files before shutting down.

- Power off terminals as employees leave.
- When adverse weather conditions appear, monitor radio stations and the National Weather Service for weather warnings and advisories.
- Send employees home early to reduce the chance of accidents involving a threat to life and limb.
- Establish snow removal procedures with the landlord or a contractor to ensure timely response to snow removal needs.
- Provide key personnel with accommodations at the nearest motel rather than sending them home.

## Response and Recovery

Personnel safety is a primary concern. Work schedules should be reduced to minimum essential operations during expected peak storm conditions and during recovery actions.

The account manager, disaster recovery manager, or other appropriate employees should be notified of site conditions, damage, or system failures.

The main problems associated with severe winter storms or blizzard conditions are the loss of power and telecommunication due to downed utility lines. Outage and recovery procedures relevant to the type of disruption experienced should be implemented.

- If problems are related to loss of power, use the procedures outlined in this section.
- If problems are related to fires and explosions, use the procedures outlined in this section.
- If conditions arise from flooding or water damages, use procedures outlined in this section.
- Key personnel can dial-up from home to monitor the operating system and its applications.
- Operate in weekend mode if weather conditions warrant it.
- Inform employees of the steps to keep fully informed of the status of return to work conditions. This may be a central recording device (voice mail) that personnel can call for up-to-date information.
- Electrical power losses may be replaced by using a rental generator. Ensure that high-quality power supply conditioning equipment is used between the generator and computer hardware.

## Tornadoes

Indiana is in a high probability tornado area. However, whereas the strikes tend to be infrequent, they also tend to be quite severe. Specific hazards include structural damage, utility outages, transportation disruptions, and resource shortages. The months of greatest concern are April through June.

Tornadoes can be destructive and pose a threat to the EDS Indiana Title XIX computer operations. Disaster conditions from tornadoes can take many forms, including the following:

- Damaged or destroyed supporting utilities, such as electrical power lines, communications lines, and other facilities
- Damage to the EDS Indiana Title XIX building, its occupants, and contents
- Disruption of transportation and highways

## Prevention

The National Weather Service is responsible for issuing warnings to the public. A tornado *warning* means that a tornado has been sighted in the area. In most cases, a tornado watch is issued before such a storm. Tune to a local radio station for tornado reports during violent weather.

During threatening weather or tornado watches, all users and system administrators should save data regularly.

## Response

The disaster response manager should obtain critical backup media from the computer room vault. They should also have a copy of the *Disaster Recovery Plan* and any site administration manuals. These will be carried until an all clear is announced.

- The facility has no formal tornado advisory method. If a tornado warning has been announced, heard over the radio, or if conditions are threatening, employees should take shelter in a stairwell or restroom. All persons seeking shelter should evacuate to the ground level floor.
- All personnel should seek shelter from windows in the interior of the building. If possible, managers should check the work area before seeking shelter to ensure that all persons have received the warning notice.
- Safe areas include rest rooms, interior rooms without windows, stairwells, or lowest floors.
- An all clear from one storm should not be the only criteria used to end take shelter precautions. Sometimes more than one tornado develops from a single storm.
- Personnel should remain in shelter until the all clear notice is given by the National Weather Service.

If damage occurs as a result of a tornado, personnel are guided by the following procedures:

- Attend to the medical and safety needs of personnel, if necessary.
- Employees should secure areas if the building is damaged during working hours
- Nonessential personnel should be released from work areas affected by the storm.
- The EDS account manager notifies the OMPP operations of the event and potential impact on the customer base. Timely updates shall be submitted to the customer keeping them informed on the state of operations.
- In the event of catastrophic damage to the facility, it may not be possible to enter the building for days. The Indianapolis Emergency Management Division, fire marshal, or other officials from the state or local government determine if the building is safe to enter.
- The communication coordinator, at the direction of the disaster response manager or account manager, contacts the disaster response, computer support, facility, and assessment coordinators or their alternates, until each position is manned. Phone lines may be out of order and necessitate that contact be made using the address list contained in this plan.
- The computer support, facility, and assessment coordinators make an initial determination of the extent of the damage. Employees should be alert to fire hazards such as broken electrical wires, damaged electrical equipment, and so forth. The assessment coordinator will make photographic evidence of damage.
- The computer support coordinator evaluates any affected hardware, estimates downtime, and reports this information to the assessment coordinator.
- The facility and computer coordinators attempt to protect hardware from the elements.
- The assessment coordinator reports to the account or disaster response manager and gives a status report of current conditions and the expected duration of the problem.
- After conferring with other senior EDS leaders, the EDS account manager determines if conditions require the declaration of a disaster. The intent of the account support staff in reacting to the situation, such as relocating part or all of their support process, is clarified. Upon declaring a state of disaster, the EDS Account manager informs the OMPP of any plans to invoke a disaster recovery plan to a backup site.
- The disaster response manager determines if the damage to hardware and applications is catastrophic enough to warrant contacting EDS Risk Management and the EDS Crisis Management

team. The disaster response manager creates a responsibility center to track all expenses associated with this event

- If a disaster is declared, the communication coordinator advises the disaster response team to assemble at the Holiday Inn – North or Hyatt Regency – Downtown. The purpose of the meeting is to develop actions. An action plan is identified based on the customer's intent and it is reviewed by the EDS leadership team.
- After an action plan is identified, the facility coordinator facilitates the necessary repairs to ensure the integrity of the structure surrounding the computer hardware.
- The assessment coordinator takes a photographic record of any visible damage.
- If a long-term structural repair is likely, move the critical business functions to the alternate processing sites.
- The computer support coordinator may find it necessary to use the expertise of vendor service personnel to establish the integrity of affected hardware. Third party maintenance providers may also be used to determine if hardware can be certifiably repaired.
- If equipment replacement is required, it is requisitioned through normal EDS channels. If the equipment is critical, an emergency requisition is necessary through the account manager.
- Segregate, but do not dispose of, irreparable hardware, as it may have to be examined by EDS Risk Management adjusters.
- If the movement of some or all of the processing capability is deemed necessary, the disaster response team leader notifies the affected account support managers.
- The disaster response team leader makes arrangements for transportation to and lodging at customer site for critical personnel if an alternate site is used, and if necessary.
- The facility coordinator ensures the primary or alternate site has the necessary environmental controls (HVAC, fire protection, and electrical power) and voice and data communication. This may involve communications with WorldCom, AT&T, Executone, Ameritech, and MCI.
- Identify the hardware necessary to meet the minimum information processing requirements for critical operations.
- If the hardware within the site is deemed unusable, or unrepairable, acquire the necessary hardware through EDS-Technical Resource Acquisition's excess equipment listing or through normal purchasing procedures.
- The disaster response team leader and computer support coordinator develop an installation schedule for the facility or at the alternate processing site for the new and relocated hardware.
- The computer support coordinator installs the hardware according to the schedule.
- Obtain any necessary operating supplies.
- The communication coordinator and computer support coordinator coordinate restoration and verification of data communication for the minimum account network to support critical operations.
- The communication coordinator requests telecommunication vendors check the integrity of the communication lines for critical hardware and functions.
- Direct requests from the account support staff for variations to the critical applications and hardware to the disaster response manager.
- The disaster response team leader and computer support coordinator develop security procedures for the new site or alternate processing site. EDS Information and Physical Security departments may assist.

## Recovery

- The disaster response team leader, computer support coordinator, and account support staff determine the synchronization point, most likely the last backup before the catastrophe.
- The computer support coordinator identifies the backup media required for recovering the operating environments and the account-owned applications and data in priority sequence.
- Recover the operating system, account-owned applications, and data in priority sequence at the new installation or alternate processing site.
- Verify the operability of the recovered operations.
- Return backup media to storage.
- Obtain account support staff verification of data recovery to the synchronization point, and after reprocessing lost data.
- The disaster response team leader instructs the affected account support managers about the need to process data that was created, modified, or deleted while information processing services were not available.
- The account will, at all times, be aware of the timeframe that the *AIM* application must be available under contractual obligations. The OMPP must be kept informed of all decisions that impact availability of services.
- If access to the facility will take more than two days, the EDS Indiana Title XIX staff will discuss relocating part or all of its support functions.
- Perform insurance and salvage activities in the area affected by the damage. Information on the specifics of this function can be obtained through EDS Risk Management.
- Segregate damaged hardware, office equipment, and so forth.
- Contact Sun maintenance to recertify and to determine the reparability of affected hardware. Segregate unsalvageable hardware. Do not dispose of any hardware until EDS scrap forms are issued by EDS Purchasing USA.
- The computer support coordinator and assessment coordinators quantify the estimated dollar loss associated to the equipment.
- Obtain EDS Risk Management insurance adjuster's authorization to replace or repair equipment.
- The assessment coordinator works with the disaster response team leader to document any losses incurred, including all loss-related expenses such as internal labor costs plus burdens, segregating premium from straight time and building repairs.
- The facility coordinator salvages all usable office equipment, files, and supplies.
- The facility coordinator should use the EDS Business Continuity Planning Guide that clearly defines actions that should be taken to facilitate recovery.
- The facility coordinator obtains a schedule and work plan for rebuilding the primary work area. An occupancy date is also determined.
- The EDS account manager confers with the OMPP about the plans to recover the site. During this discussion, all aspects of the contract are reviewed to ensure full compliance and any needed authorizations from the OMPP are in place.
- The disaster response manager and account manager communicate schedules for recovering suspended and alternate process functions with the account support staff.
- Contact EDS Real Estate to use their services to facilitate restarting business at the home site.
- Assure the primary or alternate site has the necessary environmental controls (HVAC, fire protection, and electrical power) and voice communication.

- Identify the hardware necessary to meet the information processing requirements.
- If the hardware within the site is deemed unusable, or irreparable, acquire the necessary hardware through EDS-Purchasing USA's excess equipment listing or through normal purchasing procedures.
- The disaster response team leader and computer support coordinator develop a facility installation schedule for the new and relocated hardware.
- The computer support coordinator checks the physical condition of all hardware cables prior to installation. Any cables that appear to be questionable are replaced and checked by the vendor as time allows. Questionable cabling is returned for refund using EDS TRA services.
- The computer support coordinator installs the hardware according to the schedule.
- Obtain any necessary operating supplies.
- The communication coordinator and computer support coordinator coordinates the restoration and verification of data communication to support the operations.
- The communication coordinator will request the telecommunication carriers to check the integrity of the communication lines for critical hardware and functions.
- Requests from the account support staff for variations to the applications and hardware will be directed to the disaster response manager.
- The disaster response team leader and computer support coordinator update security procedures for the primary site. EDS Information and Physical Security Departments may assist in this area.
- The disaster response team leader, computer support coordinator, and account support staff determine the synchronization point, most likely the last backup.
- The computer support coordinator identifies the backup media required for recovering the operating environments.
- The computer support coordinator identifies the backup documentation and manuals required for recovering the operating environments.
- The computer support coordinator identifies the backup media required for recovering the account-owned applications and data in priority sequence.
- Recover the operating system, account-owned applications, and data in priority sequence at the site.
- Verify the operability of the recovered operations.
- Return the backup media to storage.
- Obtain account support staff verification of data recovery to the synchronization point after reprocessing lost data.
- The disaster response manager schedules the migration from any alternate processing sites back to the primary facility.
- The EDS account manager confers with the OMPP about the plans to recover the site. During this discussion, all aspects of the contract are reviewed to ensure that full compliance and any needed authorizations from the OMPP are in place.
- All plans to recover the home site from this point on will be held with representatives of the OMPP to ensure that all scheduled dates of implementation are adhered to by all parties to avoid any breakdown in communication.
- Establish a move date in conjunction with the State.
- Establish a curfew period for changes to the operating system, data communication, support programs, production jobs, and data, so they may be backed up for migration back to the primary

facility. The disaster response team leader notifies the appropriate account supervisors of the scheduled migration.

- The necessary incremental back-up media or disks for migration are created from the alternate processing sites. Necessary application and backup media for restoration are acquired from the vaults and offsite storage.
- Verify the operability of the recovered site by testing equipment functions, software, operating system, application functions and interfaces, all voice and data telecommunication to local and remote terminals, and network interfaces.
- Coordinate the relocation of any off-site personnel back to the primary site.
- Any data processed manually by the account support staff during the period of time that the electronic data processing functions were affected will be reprocessed in the restored system.
- When systems are restored, they are backed up and the tapes stored immediately offsite.
- The disaster response team leader collects activity logs from the communication coordinator and the reports from the assessment coordinator.
- The disaster response manager and disaster response team leader analyzes the team's efforts to find ways to improve future recovery efforts.
- Based on approval of EDS Risk Management and EDS-TRA Disposition, the disaster response team leader instructs the facility coordinator to dispose of irreparable hardware.

## Technological Hazards

Technological hazards are manmade hazards that could endanger personnel safety. Although it is not feasible to address every circumstance relating to manmade disasters, this document presents circumstances of reasonable likelihood. For the EDS Indiana Title XIX account, this includes hazardous material accidents, radiological accidents, and internal water damage from overhead pipes or a roof leak.

These procedures are intended to supplement the existing EDS account orders and local instructions, held by Indianapolis for similar emergency precautions.

## Hazardous Materials

The EDS site is an area of moderate risk for hazardous materials. The primary risk in the area is from chemicals stored at a nearby water treatment facility. Employees are trained to react to potential hazards presented by this facility through material in the account policies given to all staff members.

The nearby major interstate, exposes the site to a moderate risk of a hazardous material incident. Interstate I-465 is a hazardous cargo route located approximately eight miles west of the site. This places the facility in an area of risk. Haulers of hazardous chemical, explosive, biological, and radioactive materials are regulated from traveling through the part of the city where the building is located. Specific hazards include spills, leaks, fires, and explosions due to traffic accidents or defective equipment. Any of these could result in environmental contamination, injury, or loss of life to persons coming in contact with or inhaling the material. Depending on the location of the incident, and the direction of the plume, long-term evacuation may be ordered.

### Prevention

Little can be done to prevent such an incident.

**Protective Measures**

If dangerous vapors enter the building, take shallow breaths through a cloth or towel. (The same procedure may offer some protection from smoke in a fire.) The use of a cloth is strictly a defensive measure and offers only minimal protection.

*Minimizing the Inhalation Hazard* – In a motor vehicle, close off ventilation and shut the windows. Distance yourself from the source; sightseeing at an incident of this type is an unnecessary risk.

*Minimizing the Risk of Skin Absorption* – Many toxic materials can be easily absorbed by the skin. Avoid any spilled liquid material, mist in the air, or condensed solid chemical deposit. Keep your body fully covered, including gloves and socks. When you have left the area, fully disrobe, proceed through decontamination, and redress in fresh clothing.

*Avoiding Ingestion of Toxic Substances* – Toxic substances can be ingested if the food or water supply becomes contaminated. If you learn that you will be sheltered indoors, quickly fill the bathtub or containers with a supply of uncontaminated water and turn off the intake valve to your home or building. Do not eat any food that could have become contaminated in an incident.

*Decontamination* – A person or item that has been exposed to a hazardous material is contaminated and can contaminate other people or items. For instance, if you enter your car after being exposed to a toxic substance, you will contaminate your car. Decontamination is the process of removing or neutralizing contaminants that have accumulated on people and equipment. At hazardous waste incidents, clean areas must be established and maintained and materials in contaminated areas are confined to specific hot zones.

If you believe you may be contaminated and medical assistance is not immediately available, remove all clothing, shower thoroughly, wear fresh loose warm clothing, and seek medical help. Place exposed clothing in a non-permeable container without allowing it to contact other materials, and arrange for proper disposal.

**Response**

Seeing or hearing an accident on the surrounding roads and your senses may be the first notification of an incident. Odors such as rotten fruit, rotten eggs, freshly cut grass, and so forth, are characteristic of certain hazardous materials. Some chemicals can desensitize the sense of smell after the second or third sniff. The color of smoke or flame can also identify the presence of hazardous material. Irritation to the eyes or skin is also a signal of exposure.

If caught outdoors during a hazardous materials incident, it is best to stay upstream, uphill, or upwind. Move toward a crosswind, so the wind is blowing from either the right or the left rather than directly in the face or at the back. Go at least 10 city blocks (one-half mile) from the danger area; for many incidents, go much further.

Reaction to a hazardous material incident should include the following procedural steps:

1. The State Police or Indianapolis Police and Fire Departments may make notification of a hazardous material incident occurring near the site, by telephone or emergency personnel going door-to-door.
2. Management personnel should immediately contact EDS security and get as much detail as possible from the emergency personnel.
3. If conditions warrant, precautionary protective actions, including evacuation, may be initiated. The decision to evacuate will be made by the account manager, the disaster response manager, or by direction of local municipal emergency personnel.
4. Emergency personnel may initiate protective sheltering that generally involves staying indoors, shutting all doors and windows, and shutting off the ventilation system, until the threat passes.
5. The EDS leadership team should assist local authorities as directed, including the assurance that all personnel stay indoor, or evacuate as ordered.

Precautionary evacuation procedures should include the following steps.

1. If a precautionary evacuation is ordered, nonessential personnel will be released by their supervisors. The disaster response team assembles at the Holiday Inn – North or Hyatt Regency – Downtown, if it is outside of the affected area, or another location offsite designated by the account manager that is outside the danger area.
2. If time allows, the computer support coordinator will gather the following before evacuating: Critical tapes or other media, the *Disaster Recovery Plan*, and any site administration materials.
3. If the building is evacuated during working hours, employees should secure areas where as safely possible.
4. Attend to the medical and safety needs of personnel, if necessary.
5. Upon reaching a safe area, the disaster response manager should advise the OMPP and the SHC account office of the situation on a need to know basis.
6. In the event of a major hazardous material emergency, it may not be possible to get into the building for days. The Indianapolis emergency manager or fire marshal determines if the building is safe to enter.
7. After conferring with local municipal officials and EDS leadership, the account manager determines if conditions require a declaration of a disaster. If the situation appears that it will be resolved within three calendar days, then operations at the facility should be suspended, and run in weekend mode, until access to the facility is viable.

If it appears the facility will take longer than two days to access, the account support staff will discuss relocating part or all of their development and support process. The EDS account manager, after conferring with senior EDS SHC management, informs the OMPP of any plans to invoke a disaster recovery plan and move to a backup site.

In the event the account support staff intends to relocate all or part of development and support process for the duration of the evacuation, the disaster response efforts are guided by the following procedures:

- The account manager determines the assembly site for the coordination of recovery efforts, especially if the Holiday Inn – North or Hyatt Regency – Downtown is unacceptable.
- The communication coordinator, at the direction of the disaster response manager or account manager, should contact the disaster response team or its alternates, until each position is manned. Team members are instructed to assemble at the determined site for coordination of recovery functions.
- The disaster response team must determine the level of support necessary for supporting the critical business functions of the account support staff.
- The computer support coordinator should determine what hardware and software is necessary to support the customers intended business functions. They should also determine the environmental and power requirements for this operation and inform the facility coordinator.
- The facility coordinator should determine the availability of space for the determined recovery efforts.
- Develop a skeleton implementation plan. The likelihood of meeting the EDS product support staff's requirements should then be established.
- The disaster response manager updates the account manager of the proposed action plans.
- The account manager informs the OMPP and SHC account office in Plano, Texas, of the plan and advise them of the intent of plan implementation.

- The disaster response manager determines if the situation warrants the involvement of EDS Risk Management or the Crisis Response team.
- Upon account support staff approval of the EDS action plan, the facility coordinator facilitates acquisition and build outs of the necessary space for the response and recovery efforts.
- The assessment coordinator acquires copies of news releases about the incident.
- The computer support coordinator may find it necessary to use similar, but not identical critical hardware, based on availability of excess, loaned, and open stock items from Sun or other vendors.
- The computer support coordinator should ensure that existing licensed applications and software run on the available hardware. Use of the expertise of Sun or other third party personnel is helpful in this effort.
- If equipment acquisition is required, it is acquired through EDS-Technical Resource Acquisition's excess equipment listing or requisitioned through normal EDS channels. If the equipment is critical, an emergency requisition may be necessary through the account manager.
- The assessment coordinator documents the team's efforts to acquire the necessary hardware and software internally, as they may have to be examined by EDS Risk Management adjusters.
- If an alternate processing or business site is necessary, contact EDS Real Estate to use their services to facilitate an alternate processing and alternate business site.
- Ensure the alternate site has the necessary environmental controls (HVAC, fire protection, and electrical power) and voice and data communication.
- The disaster response team leader and computer support coordinator should develop an installation schedule for the facility or at the alternate-processing site for the hardware.
- The computer support coordinator should install the hardware according to the schedule.
- Obtain any necessary operating supplies.
- The communication coordinator and computer support coordinator coordinate installation and verification of data communication for the minimum account network to support the critical operations.
- The communication coordinator requests local telecommunication vendors check the integrity of the communication lines for critical hardware and functions.
- Direct requests from the account support staff for variations to the critical applications and hardware to the disaster response manager.
- Depending on the relocation of the customer's production facilities and alternate processing sites used, the disaster response team leader arranges for transportation to and lodging at customer sites (if deemed necessary) for critical personnel.
- The disaster response team leader and computer support coordinator develop security procedures for the alternate-processing site. EDS Information and Physical Security Departments may assist.
- The disaster response team leader, computer support coordinator, and account support staff determine the synchronization point. If the critical backup media was not removed from the computer room at the time of evacuation, this is the last backup media stored at the offsite storage location.
- The computer support coordinator identifies the backup media required for recovering the operating environments.
- The computer support coordinator identifies the back-up media required for recovering the account-owned applications and data in priority sequence.

- Recover the operating system, account-owned applications, and data in priority sequence at the alternate processing sites.
- Verify the operability of the recovered operations.
- Return backup media to storage.
- Obtain account support staff verification of data recovery to the synchronization point.
- The disaster response team leader instructs the EDS area supervisors affected on the need to process data that was created, modified, or deleted while information processing services were not available.
- Obtain account support staff verification of data recovery after reprocessing lost data.

## Recovery

When the municipal or state Emergency Management coordinator or Fire Department chief has determined that the hazardous material incident conditions permit safe reentry into the site, account personnel perform the following: (this assumes that part or all of the electronic data processing functions were relocated to alternate processing sites.)

- Contact Sun maintenance to determine if recertification of maintainability is necessary.
- The assessment coordinator works with the disaster response team leader to document any losses incurred; including all loss related expenses such as internal labor costs plus burdens, segregating premium from straight time.
- The facility coordinator obtains a schedule and work plan for reoccupying the account site.
- The disaster response manager and account manager schedule the migration from any alternate processing sites to the primary facility. The account manager communicates this schedule, as well as those for restoring suspended and alternate process functions, with the account support staff.
- The EDS account manager presents the migration schedule to the OMPP for review and approval. All contractual obligations are reviewed and approved toward the implementation of the site's restoration to full productivity.
- Establish a curfew period for changes to the operating system, data communication, support programs, production jobs, and data, so they may be backed up for migration to the primary facility. The disaster response team leader notifies the appropriate EDS area supervisors of the scheduled migration.
- Create the necessary backup media for migration from the alternate processing sites. Necessary application and backup media for restoration is acquired from the computer room or offsite storage.
- Verify the operability of the recovered site by testing equipment functions, software, operating system, telecommunication, and all local terminals.
- Migrate operations in critical-alternate process-suspend order.
- Obtain account support staff verification of data migration.
- Return backup media to storage.
- Coordinate the relocation of offsite personnel and recall evacuated personnel.
- Reprocess any data processed manually by the account support staff during the period of time that the electronic data processing functions were affected in the restored system.
- When systems are restored, back up and store the backup media immediately offsite.
- The disaster response team leader collects activity logs from the communication coordinator and the reports from the assessment coordinator.

- The disaster response manager and disaster response team leader analyze the team's efforts to find ways to improve future recovery efforts.

## Universal Hazards

Universal hazards threaten the safety and well-being of a large number of people and can damage millions of dollars in property and lost business in a short period of time. Long-term effects can continue for weeks afterwards. Fears also can interrupt normal functions of a business.

Universal hazards that could impact EDS Indiana Title XIX include: bomb threats, resource failure, utility problems, structural fires and explosions, domestic disturbances, conventional or nuclear enemy attack, sabotage, and employee accidents.

Of these utility problems, fires, sabotage, employee accidents, and resource failures are considered the most significant threats to the EDS Indiana Title XIX facility.

## Utility Problems

Disruption of electrical power and communications lines is a high threat to the EDS Indiana Title XIX facility.

The loss of power to the EDS Indiana Title XIX facility can be caused by several different conditions. Typically they include the following:

- Power surge
- Power drop
- Tripped circuit breaker in power panels
- Blown fuse or tripped circuit breaker in the equipment
- Bad power supply in the equipment
- Thermal condition that automatically powers down the equipment to prevent damage
- Occurrence of a natural disaster, such as windstorm, lightning, flooding, and so forth

There is no provision for the generation of emergency power at this facility other than the two UPSs in the computer room.

The UPS in the computer room protects against all spikes and sags. It allows for an orderly shutdown of the equipment in the range of 20 minutes as the battery backup cuts in when a power loss is detected. There is software that allows for an orderly shutdown or reboot by local or remote means. This software can also be used to page a systems support person in the event of a disruption of service.

In these situations, when electrical power fails and when power is being restored, all computer operations personnel must be familiar with power up and down procedures for all devices, and with the location of the circuit breaker and thermal indicators (if applicable) for all devices.

### Prevention

Preventive measures to protect computer and communication hardware from electrical power surges caused by severe lightning storms and power spikes include circuit breakers, power strips, and the possible inclusion of UPSs. A UPS protects the Sun computer system located at the EDS account.

If conditions are threatening, such as during an electrical storm, preventive shutdown of the hardware minimizes the occurrence of power-related hardware failures (such as from spikes and sags).

Processing during intermittent power supply problems should be suspended upon approval of management, until the threat of corruption has passed.

High-quality power conditioning equipment, such as surge suppressers and UPSs are used on all workstations, personal computers, and peripherals to prevent damage from sudden power surges. Inexpensive power strips do not shunt surges or interrupt the flow of power that can allow these destructive electrical surges and spikes. As a result, internal components of the hardware fatigue and equipment can be destroyed.

## Response

When a disruption of the quality of electrical power is suspected, the EDS operations support personnel notify the disaster response manager immediately.

If a significant service interruption is suspected, the following actions should be taken:

- The communication coordinator, at the direction of the disaster response manager or account manager, contacts the facility, computer hardware, computer application, and assessment coordinators.
- The facility coordinator determines the extent of the power outage or disruption and reports this information to the assessment coordinator.
- The computer support coordinator and assessment coordinators evaluate affected information processing services and estimate downtime.
- The assessment coordinator reports to the account or disaster response manager, and gives a status report of current conditions and expected duration of the problem.
- After conferring with other EDS senior leaders and the account support staff, the account manager determines if conditions require a declaration of a disaster.
- The EDS account manager notifies the OMPP of the event and potential impact on the customer. Timely updates are submitted to the customer to keep them informed on the state of operations.
- If a disaster is declared, the communication coordinator assembles the disaster response team in a designated conference room to develop actions.
- After an action plan is identified, the facility coordinator facilitates the necessary repairs to ensure clean power to the critical hardware. If a long-term power outage is likely, a rental generator should be considered.
- The computer support coordinator may find it necessary to use the expertise of Sun or other third party service personnel to establish the integrity of affected hardware. Power surges and electric pulse modifications can affect computers in unusual ways. Do not immediately believe that a puzzling hardware problem means replacement is necessary. Attempt to restore what might ordinarily not be necessary. For example, the user interface might indicate that a device's baud rate is set for a normal position of 1200. Symptoms of the problem lead you to believe the baud rate is wrong. Reset the baud rate to 2400, or another setting, and then switch it back.
- Use a line analyzer tool to identify the type of fluctuations occurring. Information, such as the time of day or type of disruption, can help in identifying and fixing the cause of the disruption. If this device is not available through the local skilled trades, the workstation support group, EDS-Client/Server Integration Division, Troy, Mich., can perform an analysis.
- If equipment replacement is required, requisition it through normal EDS channels. If the equipment is critical, an emergency requisition is necessary through the account manager. Segregate, but do not dispose of, irreparable hardware, as it may have to be examined by EDS Risk Management adjusters.
- The computer support coordinator ensures that users investigate the integrity of the data they were working on at the time of the power fluctuation. They should also be instructed to try several

resident applications. Reloading of applications or data is prioritized based on the critical applications listed in the appendix of this manual.

- The communication coordinator requests local telecommunication vendors check the integrity of the communication lines for critical hardware and functions.
- Direct requests from the account support staff for variations to the critical applications and hardware to the disaster response manager.
- In the event of catastrophic power failure, it may be necessary for the communication coordinator to advise customer accounts, and SHC account office in Plano Texas.
- If the power fluctuation caused catastrophic hardware damage, the assessment coordinator takes a photographic record of any visible damage such as burned power strips, exploded component on system boards, and so forth.
- The disaster response team leader reports all status information to the disaster response manager.
- The disaster response manager determines if the damage to hardware and applications is catastrophic enough to warrant contacting EDS Risk Management.
- Restore the effected hardware, software, data, and communication based on the identified prioritization. The disaster response manager and account manager communicate schedules for recovering suspended and alternate process functions with the account support staff.
- The response team leader verifies recovery of all processes with the account support staff area supervisors.
- Reprocess any data processed manually by the account support staff during the period of time that the electronic data processing functions were affected in the restored system.
- When systems are restored, back up and store the media immediately offsite.
- The disaster response team leader collects activity logs from the communication coordinator and the reports from the assessment coordinator.
- The disaster response manager and disaster response team leader review the team's efforts to find ways to improve future recovery efforts.
- Perform insurance and salvage activities in the area affected by the damage. Upon the instruction of the disaster response team leader, based on approval of EDS Risk Management and EDS-TRA Disposition, the facility coordinator dispose of irreparable hardware.
- Segregate damaged hardware, office equipment, and so forth.
- Contact Sun maintenance for recertification and to determine the reparability of affected hardware. Segregate unsalvageable hardware. Do not dispose of any hardware until EDS scrap forms are issued by EDS Purchasing USA.
- The computer support coordinator and assessment coordinators quantify the estimated dollar loss associated to the equipment.
- Obtain EDS Risk Management insurance adjuster's authorization to replace or repair equipment.

## Recovery

### **Power Fluctuations**

When several computer resources, critical to operations, are plugged directly into house power or inexpensive power strips, they may be impacted by fluctuations, surges, noise, brownouts, and losses of power. Failure of these hardware devices causes short-term impact to the business functions. These critical devices are protected with interruptible power supplies to condition and transform power.

If conditions become threatening, such as in an electrical storm, preventive shutdown of the hardware minimizes the occurrence of power-related hardware failures (such as from spikes). Processing during intermittent power supply problems is suspended, until the threat of corruption has passed.

High-quality surge suppressors are used on all workstations, personal computers, and peripherals to prevent damage from sudden power surges. The building does not have its own electrical substation. Electrical wires are buried and this should eliminate some interference problems that can be caused by weather.

## Structural Fires

Fire is the most common threat to information systems personnel, resources, and operations. All personnel should be constantly aware of fire prevention measures and emergency procedures to be followed in the event of fire.

The site is a moderate risk. Specific hazards include an evacuation of the facility, destruction of hardware, media, corruption of software and firmware due to heat, and overall water and smoke damage to the facility. Fire extinguishers are present and the building is sprinkled. The building is not guarded during off hours.

The Indianapolis Fire Department protects the EDS Indiana Title XIX facility. A fire station is located 2.5 miles from the site. It is a full-time staffed department. Typical response time is 2.5 minutes. The proximity to the fire department will help prevent fire spread. EDS personnel onsite have been trained regarding fire evacuation procedures.

There are numerous A-grade portable fire extinguishers throughout the structure. They are quality pressurized water style. Several CO<sub>2</sub> extinguishers are also in the facility. Extinguisher inspections are kept current.

The EDS Indiana Title XIX facility is protected by a wet sprinkler system, using 165-degree Fahrenheit sprinkler heads.

EDS employees assume responsibility for cleanup during business hours and the evening maintenance crew typically performs custodial duties.

### Prevention

The manager of the computer room should ensure that sound housekeeping standards are maintained.

All employees should know the location and operation of the following:

- Fire extinguishers
- Work area and building exits
- Main power cutoff switches on hardware
- Smoke and heat detectors and the alarms system
- Fire alarm pull boxes

All personnel should be aware of the following fire classifications:

- *Class A* – Fires involving ordinary combustible solids, such as wood, cloth, paper, rubber, and many plastics. These fires can be extinguished with water, CO<sub>2</sub>, dry chemical, and Halon.
- *Class B* – Fires involving flammable or combustible liquids and flammable gases. These fires can be extinguished with CO<sub>2</sub>, dry chemical, and Halon – **but never with water.**

- *Class C* – Fires involving energized electrical equipment. Dry chemical or Halon should be used on computer and communication equipment. If possible, use of CO<sub>2</sub> should be avoided on computers and communication equipment. **Water should never be used in proximity to electrical boxes or equipment.**

EDS security provides instruction if asked.

#### Response

- If a fire is discovered prior to activation of smoke detectors and the fire suppression or alarm system, the person detecting fire or smoke should activate the nearest fire alarm and immediately notify the other employees if present. The alarm system should be manually activated.
- If appropriate, an attempt should be made to extinguish the fire by using a portable fire extinguisher or other immediately available method. Personnel should not undertake such an effort if safety or well being is in jeopardy.

When the fire alarm sounds, all nonessential personnel should immediately evacuate the building. Execute the following procedural steps:

- Notify local authorities immediately by dialing 911.
- Estimate the severity of the situation and place primary emphasis on the safety of personnel.
- Notify the EDS Title XIX account manager.
- Assume the fire is not in a computer, issue system shutdown commands and allow the computers to cycle down, before shutting the power off.
- If the fire is of electrical origin, immediately turn the power switches off for the particular system, then power down all the remaining systems, peripherals, and terminals. Let the hardware cycle down before turning off the main circuit breakers.
- Shut off all air-conditioning units after all computer equipment has been powered off.

In the event of fire or explosion, disaster response team members and their alternates are guided by procedures for team assignment as follows.

*Note: Safety to personnel is the highest priority. Heat, smoke, and falling debris may cause injury or loss of life. Structural damage or collapse may occur if the fire or explosion is strong enough. Panic may result in further injuries; therefore, team members need to be organized, positive examples to others.*

- All personnel should evacuate. If possible, managers should check the work area before seeking shelter to ensure that all persons have received the warning notice.
- Personnel should remain out of the site until local fire department officials give notification that they may re-enter.

If damage occurs as a result of a fire, personnel should be guided by the following procedures:

- Attend to the medical and safety needs of personnel, if necessary.
- If the building is damaged during working hours, then employees should secure areas where as safely possible.
- Release nonessential personnel from work areas affected by the fire.
- In the event of catastrophic damage to the facility it may not be possible to get into the building for days. The Indianapolis emergency manager or fire marshal determines if the building is safe to enter. The fire department may allow one of their fire fighters to retrieve requested items.

- The communication coordinator, at the direction of the disaster response manager or account manager, contacts the disaster response computer support, facility, and assessment coordinators or their alternates until each position is manned.
- The computer support, facility, and assessment coordinators make an initial determination of the extent of the damage as soon as conditions permit, if entry is allowed. They should be alert to fire hazards such as broken electrical wires, damaged electrical equipment, and so forth. The assessment coordinator makes photographic evidence of damage. The assessment coordinator reports this information to the disaster response team leader.
- The computer support coordinator evaluates any affected hardware, estimates downtime, and reports this information to the assessment coordinator.

*Note: The positive ionization of energized electronics hardware attracts smoke particles. These particles, acidic in nature, cause damage to computer boards and circuits. Therefore, it is imperative to the recovery function that these devices be shut off, if possible.*

- Preserve nonduplicated vital records located within the area, if safely possible. Because of the threat of mold attacking the paper of wet documentation, all damaged documents should be photocopied or scanned, with a priority on the critical items that cannot be easily acquired elsewhere. This should be done while the documents are within an air-conditioned environment.

*Note: Mold makes documentation unusable within 48 hours, depending on temperature, if not refrigerated.*

- Careful clerical employees photocopy documents as assigned by the disaster response team leader.
- The facility coordinator should use the EDS Business Continuity Planning Guide that clearly defines actions that should be taken to facilitate recovery.
- The facility and computer support coordinators should attempt to protect hardware from the elements and secondary damage such as water from the sprinklers. Additional water damage can be prevented by removal or blocking up.

*Note: Ensure power in area is disconnected to prevent the possibility of electrocution.*

- Remove equipment, media, and documents. Place in an air-conditioned area. Allow water to run out of equipment. Fans can be used to dry equipment. If diskettes, tapes, or other media is immersed in water when found, store them immersed in water. This allows them to be separated for cleaning and drying, and probable retention of the data contained on them.
- The assessment coordinator reports back to the account or disaster response manager and gives a status report of current conditions and expected duration of the problem.
- After conferring with other senior EDS leaders, the account manager determines if conditions require a declaration of a disaster. The intent of the account support staff in reacting to the situation, such as relocating part or all of their development and support process, is clarified.
- The account is at all times aware of the timeframe that the *AIM* application must be available under contractual obligations. The OMPP must be kept informed of all decisions that impact availability of services.
- The disaster response manager determines if the damage to hardware and applications is catastrophic enough to warrant contacting EDS Risk Management.
- If a disaster is declared, the communication coordinator assembles the disaster response team in a conference room to develop the actions to be taken. If the conference room is not habitable, the

team meets at the Holiday Inn – North or Hyatt Regency – Downtown. An action plan is identified based on the account support staff's intent and reviewed by the EDS leadership team.

- After an action plan is identified, the facility coordinator facilitates the necessary repairs to assure the integrity of the structure surrounding the computer hardware.
- If a long-term structural repair is likely, move the critical business functions to the alternate processing sites.
- The computer support coordinator may find it necessary to use the expertise of Sun or other third party service personnel to establish the integrity of affected hardware.
- If equipment replacement is required, requisition it through normal EDS channels. If the equipment is critical, an emergency requisition may be necessary through the account manager. Segregate, but do not dispose of, irreparable hardware, as it may have to be examined by EDS Risk Management adjusters.
- If the movement of some or all of the processing capability is deemed necessary, the disaster response team leader notifies the affected EDS area supervisors.
- Contact EDS Real Estate to use their services to facilitate an alternate processing and alternate business site.
- Assure the primary or alternate site has the necessary environmental controls (HVAC, fire protection, and electrical power) and voice communication.
- Identify the hardware necessary to meet the minimum information processing requirements for critical operations.
- If the hardware within the site is deemed unusable, or irreparable, acquire the necessary hardware through EDS-Technical Resource Acquisition's excess equipment listing or through normal purchasing procedures.
- The disaster response team leader and computer support coordinator develop an installation schedule for the facility or at the alternate-processing site for the new and relocated hardware.
- The computer support coordinator installs the hardware according to the schedule.
- Obtain any necessary operating supplies.
- The communication coordinator and computer support coordinator coordinate restoration and verification of data communication for the minimum account network to support the critical operations. This includes LANs and connectivity to the EDS SMC.
- The communication coordinator requests the private common carriers check the integrity of the communication lines for critical hardware and functionality.
- Direct requests from the account support staff for variations to the critical applications and hardware to the disaster response manager.
- If an alternate site is used, the disaster response team leader arranges for transportation to and lodging at customer site (if deemed necessary) for critical personnel.
- The disaster response team leader and computer support coordinator develop security procedures for the new site or alternate-processing site. EDS Information and Physical Security Departments may assist.
- The disaster response team leader, computer support coordinator, and account support staff determine the synchronization point, most likely the last back-up before the fire.
- The computer support coordinator identifies the back-up media required for recovering the operating environments.

## Recovery

- The computer support coordinator identifies the backup media required for recovering the account-owned applications and data in priority sequence.
- Recover the operating system, account-owned applications, and data in priority sequence at the new installation or alternate-processing site.
- Verify the operability of the recovered operations.
- Return backup media to storage.
- Obtain account support staff verification of data recovery to the synchronization point after reprocessing lost data.
- The disaster response team leader instructs the affected EDS area supervisors about the need to process data that was created, modified, or deleted while information processing services were not available.
- Perform insurance and salvage activities in the area affected by the damage. Information on the specifics of this function can be obtained through EDS Risk Management.
- Segregate damaged hardware, office equipment, and so forth.
- Contact Sun maintenance to recertify and determine the reparability of affected hardware. Segregate unsalvageable hardware. Do not dispose of any hardware until EDS scrap forms are issued by EDS Purchasing USA.
- The computer support coordinator and assessment coordinators quantify the estimated dollar loss associated to the equipment.
- Obtain EDS Risk Management insurance adjuster's authorization to replace or repair equipment.
- The assessment coordinator works with the disaster response team leader to document any losses including all loss related expenses such as internal labor costs plus burdens, segregating premium from straight time and building repairs.
- The facility coordinator salvages all usable office equipment, files, and supplies. The facility coordinator should use the EDS Business Continuity Planning Guide that clearly defines actions that should be taken to facilitate recovery.
- The facility coordinator obtains a schedule and work plan for rebuilding the primary work area. An occupancy date is also determined.
- The account manager confers with the OMPP about plans to recover the site. During this discussion, all aspects of the contract are reviewed to ensure that full compliance and any needed authorizations from the OMPP are in place.
- The disaster response manager and account manager communicate schedules for recovering suspended and alternate process functions with the account support staff.
- Contact EDS Real Estate to use their services to facilitate restarting business at the home site.
- Assure the primary or alternate site has the necessary environmental controls (HVAC, fire protection, and electrical power) and voice communication.
- Identify the hardware necessary to meet the information processing requirements.
- If the hardware within the site is deemed unusable or irreparable, acquire the necessary hardware through EDS-Purchasing USA's excess equipment listing or through normal purchasing procedures.
- The disaster response team leader, and computer support coordinator develops a facility installation schedule for the new and relocated hardware.

- The computer support coordinator checks the physical condition of all hardware cables prior to installation. Any cables that appear to be questionable are replaced and checked by the vendor as time allows. Questionable cabling is returned for refund using EDS TRA services.
- The computer support coordinator installs the hardware according to the schedule.
- Obtain any necessary operating supplies.
- The communication coordinator and computer support coordinator coordinates the restoration and verification of data communication to support the operations.
- The communication coordinator requests telecommunication carriers check the integrity of the communication lines for critical hardware and functions.
- Direct requests from the account support staff for variations to the applications and hardware to the disaster response manager.
- The disaster response team leader and computer support coordinator update security procedures for the primary site. EDS Information and Physical Security Departments may be of assistance.
- The disaster response team leader, computer support coordinator, and account support staff determine the synchronization point, most likely the last backup.
- The computer support coordinator identifies the backup media required for recovering the operating environments.
- The computer support coordinator identifies the backup documentation and manuals required for recovering the operating environments.
- The computer support coordinator identifies the backup media required for recovering the account-owned applications and data in priority sequence.
- Recover the operating system, account-owned applications, and data in priority sequence at the site.
- Verify the operability of the recovered operations.
- Return backup media to storage.
- Obtain account support staff verification of data recovery to the synchronization point after reprocessing lost data.
- The disaster response manager schedules the migration from any alternate processing sites back to the primary facility.
- The EDS account manager confers with the OMPP about the plans to recover the site. During this discussion, all aspects of the contract are reviewed to ensure that full compliance and any needed authorizations from the OMPP are in place.
- Representatives of the OMPP hold all plans to recover the home site from this point on to ensure that all scheduled dates of implementation are adhered to by all parties and all contractual obligations are discussed and approved.
- Establish a move date in conjunction with the State.
- Establish a curfew period for changes to the operating system, data communication, support programs, production jobs, and data, so they may be backed up for migration to the primary facility. The disaster response team leader notifies the appropriate account supervisors of the scheduled migration.
- Create the necessary incremental backup media or disks for migration from the alternate processing sites. Necessary application and backup media for restoration are acquired from the vaults and offsite storage.

- Verify the operability of the recovered site by testing equipment functions, software, operating system, application functions and interfaces, all voice and data telecommunication to local and remote terminals, and network interfaces.
- Coordinate the relocation of offsite personnel to the primary site.
- Any data processed manually by the account support staff during the period of time that the electronic data processing functions were affected must be reprocessed in the restored system.
- When systems are restored, back them up and store the backup media immediately offsite.
- The disaster response team leader collects activity logs from the communication coordinator and the reports from the assessment coordinator.
- The disaster response manager and disaster response team leader analyze the team's efforts to find ways to improve future recovery efforts.
- Upon the instruction of the disaster response team leader, based on approval of EDS Risk Management and EDS-TRA Disposition, the facility coordinator disposes of irreparable hardware.

## **Civil Disturbances**

A civil disturbance is a situation that could include strikes, student demonstrations, mob demonstrations, terrorism, riots, or other forms of activity by groups that may deny access to or egress from information systems facilities. Civil disturbance could also involve sabotage or vandalism to the building, computer equipment, and communications facilities. A likely source would be non-organized, urban-based unrest, or an organized disruption from union sources that grows out of control.

This site is at moderate risk for civil disturbances. The Indianapolis City Police Department says there is an increasing trend to have problems in this area.

Large-scale civil disturbances can result in costly property damage that may also result in diminished operating ability. Damage to utilities may cause disruption of services for several days. Fear and reluctance on the part of personnel to enter areas perceived to be dangerous may interrupt the normal functions of the computing resources.

## **Conventional or Nuclear Attack**

This site is at moderate risk for conventional or nuclear attack. Indianapolis is an economic and manufacturing center; therefore, it is considered a prime target. Crane Naval Surface Warfare Center is located in Indiana. Camp Atterbury is an Indiana Army National Guard aviation facility located southeast of Indianapolis.

**Prevention** The EDS account cannot prevent a radiological incident.

**Response** Use procedures outlined under hazardous materials in this section.

If conditions arise that a total disaster is declared, use procedures outlined in this section.

In addition:

- Key personnel can dial-up from home to monitor the operating system and its applications.
- Employees should be informed what steps to take to keep fully informed on the status of return to work conditions. For example, a central recording device (voice mail) could relay up-to-date information.

## Computer Resource Failures

This site is at moderate risk of computer resource failures. Critical hardware pieces are integrated and unique. They do not offer opportunities to migrate workloads in the event of a resource failure. Resources are well maintained, and the operators are familiar with repair and maintenance procedures.

### File Server Head Crash

A file server head crash is a moderate risk. Critical data is mirrored to redundant disks. In case of hard drive failure, the servers will use the mirrored disk(s) automatically. Backing the system up is the best method to reduce the impact of a disk crash. Redundant or duplicate backups can be used successfully, especially if a software bug is suspected rather than a hardware failure. Maximum allowable downtimes are integrated into the vendor support requirements.

#### Prevention

Backing up the system is the most prudent method to mitigate the effect of a disk crash. Redundant or duplicate backups can be used successfully, especially if the System Administrator suspects a software bug rather than a hardware failure. If the hardware failure affects the back-up copy, the redundant backup's integrity remains intact.

#### Response and Recovery

EDS recommends using the following procedures to resolve a disk head crash on the file server or on another critical PC:

1. Obtain a copy of the vendor's system and network administration manual.
2. Replace any broken hardware.
3. The EDS system administrator recreates the system from the last backups.
4. Dismount the file system.
5. Check that the file system is dismounted.
6. Remake the file system on the disk.
7. Check that the file system was properly remade.
8. Mount the file system on a temporary mount point.
9. Restore the contents of the back-up tape.
10. Dismount the system from the temporary mounting point.
11. Check the file system for inconsistencies.
12. Mount the file system at its permanent mounting point.

## Employee Accidents

This site is at moderate risk for employee accidents because of the number of interacting support organizations that share critical areas.

## Sabotage

This site is at moderate risk for sabotage because it is a shared facility. To limit vulnerability to sabotage, observing good security practices and warnings of potential sabotage activity. Access control and positive employee identification procedures are enforced during times of possible sabotage or terrorist activity.

An act of sabotage may result in destruction, damage, or denied use of computer resources, the building housing them, or supporting utilities.

## Prevention

The examination of existing safeguards of personnel screening do not reveal any adverse personnel findings. Some ways to prevent sabotage include the following:

- Reduce target accessibility and vulnerability and allow only authorized employees access to critical areas.
- Use built-in protection on hardware and in purchased software for protection: locks, password protection, and so forth.

Another method of sabotage is less noticeable—employee disregard of system usage and the resulting consequences. OMPP and EDS' leadership should be aware of intentional use of this means of sabotage that includes the following:

- *Failure to end system session* – A user may fail to completely logoff from an application or systems session when leaving their work area even temporarily. A saboteur may take advantage of the situation to alter or copy data or to access data to which he or she does not ordinarily have access. Examples of this type of accident range from access to an otherwise inaccessible system to the use of data passed on to a third party in the commission of industrial espionage.
- *Disclosure of password* – Passwords should be kept secret unless the OMPP or EDS decides otherwise. A system administrator can be empowered to retain a secure log of employee passwords; a person in the leadership chain can also do this (such as a supervisor). The method by which this second copy is retained, however, can lead to another source of sabotage. If a second copy is retained on hard-copy, it is ultimately an easily accessible document, either through break-in of its storage area (a desk drawer, a filing cabinet, or a secure data set) or access to it through careless storage (such as hard copy left on a desk, a filename, or dataset written down in a conspicuous place). EDS recommends that the OMPP—with the aid of EDS—work out a back-up or second copy method agreeable to both parties and that works well for both the user and the system or application.
- *Virus Infection* –Unauthorized software may not be loaded onto a PC or the LAN. Routine audits are performed for such software and it is removed. Virus protection scans automatically execute at PC and LAN startup.
- *Theft* – Theft is a form of sabotage. Physical site security measures minimize risk of theft. Routine inventory audits account for all assets. This is a low-risk area.

OMPP and EDS leaders should inform employees of the consequences of writing down their password(s) near their PCs or recording their password in conjunction with their name.

A system of informing the employee's supervisor or system administrator may be the best solution.

## Response and Recovery

The following steps are recommended if there is reason to suspect that a node on the network or part of the network has been sabotaged by another employee, or a hacker who illegally entered the network:

1. The communication coordinator dispatches the computer support coordinator to determine the extent of damage. The communication coordinator determines the following:
  - How many nodes are affected?
  - Does the damage prevent the user from getting work done?
  - Is the damage spreading to other nodes?
2. If the damage is spreading to other nodes on the network, the computer support coordinator immediately disconnects the sabotaged nodes from the network.
3. The computer support coordinator reports back to the disaster response manager with its findings.

4. The disaster response manager contacts the account manager to determine if a disaster is to be declared.
5. If a disaster is declared, the communication coordinator contacts the disaster response team, and requests that they assemble in an available conference room.
6. Develop an action plan is developed between the team members. When established, the account manager contacts the OMPP and SHC account office in Plano, Texas, with the findings and course of action. The level disclosure of this incident should be discussed between the account manager and senior management. The account manager expresses that procedures require that EDS Information Security be contacted at a minimum.
7. The EDS account manager informs the OMPP within the contractually obligated timeframe (24 hours), of the state of operations and plans to overcome the situation.
8. The disaster response manager determines if the damage to hardware and applications is catastrophic enough to warrant contacting EDS Risk Management and the EDS Crisis Management team. The disaster response manager creates a responsibility center to track all expenses associated to this event
9. The communication coordinator contacts EDS Information Security and advise them of the situation.
10. If the damage to the nodes cannot be repaired, erase all data off the disk and reload the operating system and user data. If the damage is to hardware, segregate but do not dispose of the devices. Acquire replacements through normal EDS purchasing methods, with priority on critical operations.

*Note: If reloading data from backups, make sure corrupt or sabotaged data are not reloaded.*

11. Try to determine how and when the network was sabotaged and take the appropriate steps to ensure it cannot happen again. Follow the guidelines and recommendations of EDS Information Security.
12. Assure that hierarchical security is established on all files and nodes.
13. Collect activity logs from the communication coordinator and the reports from the assessment coordinator
14. The disaster response manger and disaster team leader analyze the teams' efforts to find ways to improve future recovery efforts.
15. On approval from EDS Information Security, EDS Purchasing, and the account manager, the facility coordinator disposes of any affected hardware.

## **Bomb Threats**

This is a medium risk site. All bomb threats must be assumed to be real. Caution is paramount to prevent panic. Employee general safety is the first priority.

### **Prevention**

Employees manning any central telephone activities should be familiar with the procedures, as the phone lines are likely targets for bomb threat calls.

### **Response and Recovery**

- Keep the person talking. Stay calm and listen. Gather all the information possible. Threat calls are often brief so do not interrupt.
- Get a supervisor or coworker's attention and let them know what's happening. Pass a note to call the Police at 911, if possible.
- Pretend you are having difficulty hearing and keep the caller talking.

- If the caller is agreeable to conversation, ask the following questions:
  - When will the bomb go off?
  - Where is it now?
  - What does it look like?
  - How much time is left?
  - What kind of bomb is it?
  - Who was responsible for placing it?
  - How do you know so much about the bomb?
  - Why was the bomb set?
  - Who are you?
  - Where are you?
- Gather the following about the caller:
  - Adult: \_\_\_\_ Juvenile: \_\_\_\_ Male: \_\_\_\_ Female: \_\_\_\_
  - Describe caller's voice
  - Describe background noises
  - If the building is occupied, let the caller know that a bomb could cause injury or death.
- Notify a manager, EDS Security, and local law enforcement officials immediately.
- Do not discuss this with others, except as instructed by a manager, EDS security officer, or local authorities.
- Write out the message.
- Instruct personnel to report any unusual package, box, briefcase, or container in their immediate area.
- Limit the use of two-way radios and telephones. Shut off pagers. Shut down modems and any other devices transmitting radio or microwaves.
- Evacuate the site upon instruction from a manager, EDS Security, Indianapolis city police, or Indiana State Police personnel.
- After evacuation, management should prevent re-entry, and keep all personnel 500 yards from the building to prevent possible injury from flying debris.

## **Total Destruction**

This section provides contingency plans for a disaster that results in total destruction of the account site.

The following is a list of some possible consequences of a disaster affecting the account.

- Damaged or destroyed supporting utilities.
- Damaged or destroyed electrical power lines.
- Damaged or destroyed communication lines and facilities.
- Damage to the EDS building, its occupants, and contents.
- Disruption of transportation and highways.

Business losses can include complete loss of the facility, and the loss of vital records.

### **Response**

If damage occurs as a result of a disaster, personnel must heed the following procedures:

- Attend to the medical and safety needs of personnel.

- Secure areas (where safely possible) if the building is damaged during working hours.
- Release nonessential personnel from work areas affected by the catastrophe.
- The EDS account manager notifies the OMPP operations of the event and potential impact on the customer base. Timely updates are submitted to the customer keeping them informed of the state of operations.
- In the event of catastrophic damage to the facility, it may not be possible to get into the building for days. The Indianapolis Emergency Manager (Fire Marshall) or other officials from the state or local government will determine if the building is safe to enter.
- The communication coordinator, at the direction of the disaster response manager or account manager, contacts the disaster response computer support, facility, and assessment coordinators or their alternates, until each position is manned. Phone lines may be out of order necessitating that direct contact be made using address lists contained in the Indiana interChange Business Continuity Plan (BCP).
- The computer support, facility, and assessment coordinators make an initial determination of the extent of the damage. Be alert to fire hazards such as broken electrical wires, damaged electrical equipment, and so forth. The assessment coordinator makes photographic evidence of damage.
- The computer support coordinator evaluates any affected hardware, estimates downtime, and gives this information to the assessment coordinator.
- The facility and computer coordinators attempt to protect hardware from the elements.
- The assessment coordinator reports to the account or disaster response manager, and gives a status report of current conditions and expected duration of the problem.
- After conferring with other senior EDS leaders, the EDS account manager determines if conditions require a declaration of a disaster. The intent of the account support staff in reacting to the situation, such as relocating part or all of their support process, will be clarified. On declaring a state of disaster, the EDS account manager informs the OMPP within the contractually obligated timeframe (24 hours), of any plans to invoke a disaster recovery plan and move to a backup site.
- The disaster response manager determines if the damage to hardware and applications is catastrophic enough to warrant contacting EDS Risk Management and the EDS Crisis Management team. The disaster response manager creates a responsibility center to track all expenses associated with this event.
- If a disaster is declared, the communication coordinator advises the disaster response team to assemble at the Holiday Inn – North or Hyatt Regency - Downtown. The purpose of the meeting is to develop actions. An action plan is identified based on the customer's intent and reviewed by the EDS leadership team.
- After an action plan is identified, the facility coordinator facilitates the necessary repairs to assure the integrity of the structure surrounding the computer hardware.
- The assessment coordinator makes a photographic record of visible damage.
- If a long-term structural repair is likely, moving critical business functions to the alternate processing sites is necessary.
- The computer support coordinator may find it necessary to use the expertise of vendor service personnel to establish the integrity of affected hardware. Third party maintenance providers may also be used to determine if hardware can be certifiably repaired.
- If equipment replacement is required, it will be requisitioned through normal EDS channels. If the equipment is critical, an emergency requisition may be necessary through the account manager.

- Segregate, but do not dispose of, irreparable hardware, as it may have to be examined by EDS Risk Management adjusters.
- The disaster response team leader notifies the affected account support managers if the movement of some or all of the processing capability is deemed necessary.
- The disaster response team leader arranges for transportation to and lodging at the customer site (if deemed necessary) for critical personnel if an alternate site is used.
- Follow the instructions in *Section 7*, for steps to facilitate alternate processing and business sites.
- The facility coordinator assures the primary or alternate site has the necessary environmental controls (HVAC, fire protection, and electrical power) and voice and data communication. This may involve interfacing with AT&T, Executone, SBC, and MCI.
- Identify the hardware necessary to meet the minimum information processing requirements for critical operations.
- Acquire the necessary hardware through EDS-Technical Resource Acquisition's Excess Equipment Listing or through normal purchasing procedures if the hardware within the site is deemed unusable, or irreparable.
- The disaster response team leader and computer support coordinator develop an installation schedule for the facility or at the alternate-processing site for the new and relocated hardware.
- The computer support coordinator installs hardware according to the schedule.
- Obtain any necessary operating supplies.
- The communication coordinator and computer support coordinator coordinate the restoration and verification of data communication for the minimum account network to support the critical operations.
- The communication coordinator requests that telecommunication vendors check the integrity of the communication lines for critical hardware and functionality.
- Direct requests from the account support staff for variations to the critical applications and hardware to the disaster response manager.
- The disaster response team leader and computer support coordinator develop security procedures for the new site or alternate-processing site. EDS Information and Physical Security departments may assist in this area.
- The disaster response team leader, computer support coordinator, and account support staff determine the synchronization point, most likely the last back up before the catastrophe.
- The computer support coordinator identifies the backup media required for recovering the operating environments, as well as the account owned applications and data in priority sequence.
- Recover the operating system, account-owned applications, and data in priority sequence at the new installation or alternate-processing site.
- Verify the operability of the recovered operations.
- Return backup media to storage.
- Obtain account support staff verification of data recovery to the synchronization point after reprocessing lost data.
- The disaster response team leader instructs the account support managers affected about the need to process data, which was created, modified, or deleted while information-processing services were not available.

- The account must be aware at all times of the timeframe that the IndianaAIM application must be available under contractual obligations. The OMPP must be informed of all decisions made that will have an impact on availability of services.

**If it will take longer than two days to access to the facility, the EDS Indiana Title XIX staff may choose to relocate part or all of its development and support process.**

#### Recovery

- Perform insurance and salvage activities in the area affected by the damage. Information on the specifics of this function can be obtained through EDS Risk Management.
- Segregate damaged hardware, office equipment and so forth.
- Contact Sun Maintenance to recertify and determine the reparability of affected hardware. Segregate unsalvageable hardware. Do not dispose of any hardware until EDS scrap forms are issued by EDS Purchasing USA.
- The computer support coordinator and assessment coordinators quantify the estimated dollar loss associated to the equipment.
- Obtain EDS Risk Management insurance adjuster's authorization to replace or repair equipment.
- The assessment coordinator works with the disaster response team leader to document any losses incurred, including all loss-related expenses such as internal labor costs plus burdens, segregating premium from straight time, and building repairs.
- The facility coordinator salvages all usable office equipment, files, and supplies. The facility coordinator uses the EDS Business Continuity Planning Guide that clearly defines actions that should and should not be taken to facilitate recovery of property.
- The facility coordinator obtains a schedule and work plan for rebuilding the primary work area. An occupancy date will also be determined.
- The EDS account manager confers with the OMPP counterpart about the forthcoming plans to recover the site. During this discussion, all aspects of the contract are reviewed to ensure that full compliance and any needed authorizations from the OMPP are in place.
- The disaster response manager and account manager communicate schedules for recovering suspended and alternate process functions with the account support staff.
- Contact EDS Real Estate to facilitate restarting business at the home site.
- Assure the primary or alternate site has the necessary environmental controls (HVAC, fire protection, and electrical power) and voice communication.
- Identify the hardware necessary to meet the information processing requirements.
- If the hardware within the site is deemed unusable, or irreparable, acquire the necessary hardware through EDS-Purchasing USA's Excess Equipment Listing or through normal purchasing procedures.
- The disaster response team leader and computer support coordinator develop a facility installation schedule for the new and relocated hardware.
- The computer support coordinator checks the physical condition of all hardware cables before installation. Any cables that appear to be questionable are replaced and checked by the vendor as time allows. Questionable cabling is returned for refund using EDS TRA services.
- The computer support coordinator installs the hardware according to the schedule.
- Obtain any necessary operating supplies.
- The communication coordinator and computer support coordinator coordinate the restoration and verification of data communication to support the operations.

- The communication coordinator requests that telecommunication carriers check the integrity of the communication lines for critical hardware and functions.
- Requests from the account support staff for variations to the applications and hardware are directed to the disaster response manager.
- The disaster response team leader and computer support coordinator update security procedures for the primary site. EDS Information and Physical Security Departments may assist in this area.
- The disaster response team leader, computer support coordinator, and account support staff determine the synchronization point, most likely the last backup.
- The computer support coordinator identifies the backup media required for recovering the operating environments.
- The computer support coordinator identifies the back-up documentation and manuals required for recovering the operating environments.
- The computer support coordinator identifies the backup media required for recovering the account-owned applications and data in priority sequence.
- Recover the operating system, account-owned applications, and data in priority sequence at the site.
- Verify the operability of the recovered operations.
- Return backup media to storage.
- Obtain account support staff verification of data recovery to the synchronization point and after reprocessing lost data.
- The disaster response manager schedules the migration from any alternate processing sites back to the primary facility.
- The EDS account manager confers with the OMPP counterpart about the plans to recover the site. During this discussion, all aspects of the contract are reviewed to ensure that full compliance, and any needed authorizations from the OMPP, will be in place.
- Communicate all plans to recover the home site with representatives of the OMPP to ensure that all scheduled dates of implementation are adhered to and to avoid any breakdown in communications.
- Establish a move date in conjunction with the OMPP.
- Establish a curfew period for changes to the operating system, data communication, support programs, production jobs, and data, so they may be backed up for migration to the primary facility. The disaster response team leader notifies the appropriate account supervisors of the scheduled migration.
- Create the necessary incremental backup media or disks for migration from the alternate processing sites. Acquire the necessary application and backup media for restoration from the vaults and offsite storage.
- Verify the operability of the recovered site by testing equipment functions, software, operating system, application functions, and interfaces, all voice and data telecommunication to local and remote terminals, and network interfaces.
- Coordinate the relocation of any offsite personnel to the primary site.
- Reprocess any data that was processed manually by the account support staff during the time the electronic data processing functions were affected in the restored system.
- Back up and store the tapes offsite immediately when systems are restored.
- The disaster response team leader collects activity logs from the communication coordinator and reports from the assessment coordinator.

- The disaster response manager and disaster response team leader analyze the team's efforts to find ways to improve future recovery efforts.
- On the instruction of the disaster response team leader, based on approval of EDS Risk Management and EDS-TRA Disposition, the facility coordinator disposes of irreparable hardware.

## **Appendix D: Disaster Recovery Agreement**

---

The following are excerpts from the *State of Indiana Request for Proposals for Medicaid Services*, published as *Indiana State Document RFP#F1-8-1648*. These excerpts are now part of the agreement between the state of Indiana and EDS, and document EDS responsibilities in the event of a disaster.

*Section 40, subsection 42.630*, pages 40-145 through 40-146 include the following:

- SOC-29** Demonstrate an ability to meet back-up requirements by submitting and maintaining a Disaster Recovery Plan that addresses:
- Checkpoint/restart capabilities
  - Retention and storage of back-up files and software
  - Hardware back-up for the servers
  - Hardware back-up for data entry equipment
  - Network back-up for telecommunications
- SOC-30** Provide back-up processing capability at a remote site from the Contractor's primary site such that normal payment processing and other system and services, deemed necessary by the State, can continue in the event of a disaster or major hardware problem at the primary site.
- SOC-31** Demonstrate a disaster recovery capability no less than every two (2) calendar years in accordance with *45 CFR 95.621 (f)*.
- SOC-32** In the event of a catastrophic or natural disaster, resume normal business functions at the earliest possible time, not to exceed thirty (30) calendar days.
- SOC-33** In the event of other disasters caused by such things as criminal acts, human error, malfunctioning equipment or electrical supply, resume normal business functioning at the earliest possible time, not to exceed ten (10) calendar days.

### ***Coordination Activities***

- SOC-34** Develop coordination methods for required system operational activities with other Contractors, including back-ups of information sent or accepted.
- SOC-35** Provide accesses to the ITF for other Contractors when changes are being tested that involve them.
- SOC-36** Plan and coordinate disaster recovery activities with other Contractors.



## Appendix E: Disaster Recovery Project Plan

The following Disaster Recovery Project Plan would be executed if a disaster was declared. Upon completion of this project plan, essential services would be restored to the EDS Indiana Title XIX account. When that status has been achieved, further plans would have to be developed to restore the account to Normal Business Operations. That plan would depend upon the specifics of the disaster and the decisions made by the local Crisis Management team.

### Disaster Recovery Project Plan

Task ID	Task Name	Duration	Start Date	Finish Date	Predecessors	Resource Names
1	Disaster is declared.	0	D+0	D+0		Crisis Mgt team
2	Obtain UNIX backups at Iron Mountain, send backups to Plano	1 day	D+0	D+1	1	Operating Environ Team
3	Obtain NT LAN backups at Iron Mountain, send backups to ISC alternate work site.	1 day	D+0	D+1	1	Operating Environ Team
4	Restore UNIX operating system, application and data at Plano	5 days	D+1	D+6	1,2	Operating Environ Team
5	Obtain LAN hardware, install at ISC alternate work site	1 day	D+1	D+2	1	Operating Environ Team
6	Restore LAN environment, front end and security at ISC alternate work site.	4 days	D+2	D+6	1,3,5	Operating Environ Team
7	Verify IndianaAIM application integrity	1 day	D+6	D+7	1,2,3,4,5,6	Applications Team
8	Restore Delaware Title XIX application and data	5 days	D+1	D+6	1,2	Operating Environ Team
9	Verify Delaware Title XIX application integrity	1 day	D+6	D+7	1,2,3,4,5,6,8	Operating Environ Team
10	Redirect critical voice and data circuits to ISC alternate work site	2 days	D+1	D+3	1	Telecommunications team
11	Notify Global Purchasing; procure PCs, other critical equipment	4 days	D+1	D+5	1	Logistical Support Team
12	Install PCs, other critical equipment at ISC alternate work site.	2 days	D+6	D+7	1,11	Logistical Support Team
13	Connect voice, data circuits in ISC alternate work site	3 days	D+4	D+7	1,10	Telecommunications team
14	Relocate Manual Processing at ISC alternate work site	6 days	D+1	D+7	1	Manual Processing Team
15	Restore Output processing capability at alternate work site	6 days	D+1	D+7	1	Output Processing Team
16	Relocate Logistical support at ISC alternate work site	6 days	D+1	D+7	1	Logistical Support Team
17	Disaster Recovery complete	7 days	D+0	D+7	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	All Disaster Recovery Teams



## Appendix F: Severity 1 Systems

---

The following systems are critical, and the criteria for disaster are shown below for each system.

### Chart of Severity 1 Systems

Production Environment Manager	Severity 1 System	Criteria for Disaster
	Eligibility Verification System	If system is down more than two hours between 5 a.m. and 10 p.m.; or if the system is down more than four hours between 10:01 p.m. and 4:59 a.m.
	Electronic Claims Submission	If system is down more than two hours between 5 a.m. and 10 p.m.; or if the system is down more than four hours between 10:01 p.m. and 4:59 a.m.
	Provider Payments	If weekly provider payments are not complete by 5 p.m. Tuesday.
	Interchange Online System	If system is down more than four hours between 6 a.m. and 6 p.m., Monday through Friday.



## Glossary

---

AIM System or "IndianaAIM"	Previous names for the primary computer software application that processes Medicare claims for the State of Indiana. The current name of the application is the <i>Indiana interChange System</i> .
Alternate processing site	The location where EDS computer hardware and networking services are utilized to recover application software and data so information processing ability is restored after a disaster. Also called the <i>recovery site</i> .
Alternate work site	A temporary location where EDS personnel from the Indiana Title XIX account may work in the event their normal work location becomes uninhabitable. Currently, all Indiana Solution Centre sites in Indiana are, by documented agreement, available for use by the EDS Indiana Title XIX account as alternate work sites.
Business continuity plan	A documented set of practices that mitigates risk, assures the availability of essential services for EDS and its clients, and provides for the safety and welfare of our employees during a disaster. The Business Continuity Plan has 3 primary components – The Crisis Management Plan, The Disaster Recovery Plan, and the Business Resumption Plan.
Business resumption plan	A documented process to restore EDS technical and business services to a normal level of functionality after a disaster.
Contingency management	Planning for the recovery of business and service functionality after a disruption. Includes a plan to restore essential, minimum level services and a plan for the return to normal business operations.
Contingency management teams	Teams charged with the responsibility to implement recovery processes after a disaster. There are normally 6 Contingency Management Teams, each to address recovery efforts in one of the following areas : Operating Environment, Telecommunications, Applications, Manual Processing, Output Processing and Logistical Support.
Crisis management	Actions taken to immediately respond to a potential disaster situation that threatens EDS personnel, EDS or client assets, or impairs the ability of EDS to deliver products or services to the client.
Crisis management team	A team charged with the responsibility to oversee all activities related to the Business Continuity process. This team has the authority to declare a disaster, invoke the Disaster Recovery and Business Resumption plans, direct the activities of the Contingency Management Teams and report the status of the recovery by utilizing the Response To Operational Problems (RTOP) process.
Disaster	Any situation or condition that may threaten EDS personnel, EDS or client information or assets, or impairs the ability of EDS to deliver products or services to the client.
Disaster recovery plan	A documented process to restore those EDS technical and business services that are essential to the short-term survival of the client immediately following a disaster. These services are intended to provide minimal levels of functionality while further efforts are in progress that are designed to restore all functionality to normal business operational levels.

Indiana interChange system	The current name of the primary computer software application that processes Medicare claims for the Indiana Title XIX client. Previously known as the <i>AIM</i> system or the <i>IndianaAIM</i> system.
Indiana Title XIX	The EDS client for this business unit, and the subject of this Business Continuity Plan.
Initial response team	A team charged with the responsibility to investigate all reported potential disaster situations. This team has the authority to utilize any necessary personnel and/or resource to determine if the situation can be resolved by utilizing standard operating procedures. If this team determines that standard operating procedures will not resolve the problem, they are responsible for contacting the Local Crisis Management Team and briefing them on the situation.
Recovery site	The location where EDS computer hardware and networking services are utilized to recover application software and data so information processing ability is restored after a disaster. Also called the <i>alternate processing site</i> .
Response to operational problems (RTOP)	The Response To Operational Problems (RTOP) process is the official EDS mechanism for reporting problems that impact the client. In the case of a potential or actual disaster situation, it is the responsibility of the Local Crisis Management Team to initiate and maintain a status report on the situation by utilizing the RTOP process.

# Index

## **B**

Business Continuity Plan Maintenance ... 5-1

## **C**

Contingency Management Teams ..... 6-2  
     Applications..... 6-2  
     Logistical Support..... 6-3  
     Manual Processing..... 6-2  
     Operating Environment ..... 6-2  
     Output Processing..... 6-2  
     Telecommunications..... 6-2  
 Corporate Crisis Management Office ..... 6-2  
 Crisis Management ..... 2-1  
     Assembling the Contingency  
         Management Teams..... 2-7  
     Criteria for Declaring a Disaster..... 2-5  
     Emergency Action Responses ..... 2-1  
     How to Utilize This Manual ..... 2-3  
     Initiate Disaster Response..... 2-6  
 Crisis Management Team ..... 6-1

## **D**

Disaster Recovery ..... 3-1  
     Applications..... 3-8  
     Claims..... 3-10  
     Client Services..... 3-13  
     Data Entry..... 3-11  
     Database Administration ..... 3-2  
     Electronic Solutions Help Desk..... 3-15  
     Finance ..... 3-8  
     HCBS Waiver & Hospice..... 3-16  
     Indiana Interchange Support..... 3-8  
     Local Area Network ..... 3-1  
     Logistical Support..... 3-13  
     Managed Care..... 3-18  
     Manual Processing..... 3-10  
     Office Equipment Recovery ..... 3-20  
     Operating Environment ..... 3-1

Output Processing..... 3-11  
 Resolutions & Adjustments ..... 3-9  
 Telecommunications..... 3-7, 4-7  
 Third Party Liability ..... 3-19  
 UNIX ..... 3-1

## **E**

EDS Business Continuity Policy ..... 1-1

## **F**

Forms & Tools..... 7-1

## **I**

Initial Response Team ..... 6-1

## **R**

Response To Operational Problems (RTOP)  
     process ..... 2-4, 6-1  
 Resumption of Normal Business ..... 4-1  
     Applications..... 4-7  
     Claims..... 4-10  
     Client Services..... 4-16  
     Data Entry..... 4-11  
     Database Administration ..... 4-2  
     Electronic Solutions Help Desk..... 4-18  
     Finance ..... 4-8  
     HCBS Waiver & Hospice..... 4-19  
     Indiana Interchange Support..... 4-7  
     Local Area Network ..... 4-1  
     Logistical Support..... 4-16  
     Managed Care..... 4-21  
     Manual Processing..... 4-10  
     Office Equipment Recovery ..... 4-23  
     Operating Environment ..... 4-1  
     Output Processing..... 4-11  
     Provider Enrollment ..... 4-9  
     Third Party Liability ..... 4-22  
     UNIX ..... 4-1